IKR Publishers

IKR Journal of Economics, Business and Management (IKRJEBM)
Journal homepage: https://ikrpublishers.com/ikrjebm/
Volume-2, Issue-4 (July-August) 2026
OPEN ACCESS
ISSN: 3107-8052 (Online)

Adversarial Machine Learning in Smart Grid Intrusion Detection: A Review of Threat Models, Defences, and Scada-Specific Vulnerabilities in Developing Economies

Ezirim Kelechi ThankGod[1*], Aniugo Victor Onyekachi[2], Sani Abubakar Muhammed[3], Nwaokolo Ikechukwu Frank[4], Obi Obichukwu Immanuel[5], Okoronkwo Iheanyi Chinedu[6] & Aminu Momoh[7]

[1,2,3,4,5,6]Mechatronics Engineering Department; Federal University of Technology, Owerri, Imo State, Nigeria

[7]Transmission Company of Nigeria, Akangba Sub-Region, Lagos State, Nigeria

DOI:*10.5281/zenodo.21878131*

ARTICLE INFO

Article history:
Received : 15-07-2026
Accepted : 24-07-2026
Available online : 10-08-2026

Citation: Ezirim, K. T., Aniugo, V. O., Sani, A. M., Nwaokolo, I. F., Obi, O. I., Okoronkwo, I. C., & Aminu, M. (2026). Adversarial Machine Learning in Smart Grid Intrusion Detection: A Review of Threat Models, Defences, and Scada-Specific Vulnerabilities in Developing Economies. *IKR Journal of Economics, Business and Management (IKRJEBM), 2*(4), 1-4.

ABSTRACT **Review Article**

Smart grids in developing economies are surprisingly but rapidly adopting Machine Learning (ML) for Intrusion Detection Systems (IDS) to secure Supervisory Control and Data Acquisition (SCADA) networks. However, the same Machine Learning (ML) models are detrimentally vulnerable to Adversarial Machine Learning (AML) attacks that manipulate input data in order to evade detection. This review examines AML threat models, defense mechanisms, and SCADA-specific vulnerabilities with emphasis on resource-constrained environments in developing economies. A total of 52 studies from 2018-2025 were analyzed and categorized attacks into evasion, poisoning, and model extraction. Key findings indicate that developing economies face compounded risk due to legacy SCADA, limited cybersecurity expertise, and poor data quality. We propose a tiered defense framework combining adversarial training, anomaly detection, and SCADA protocol-aware filtering. Future research should prioritize lightweight defenses, domain adaptation, and threat intelligence sharing tailored to low-bandwidth grids.

Keywords: Adversarial Machine Learning, Smart Grid, Intrusion Detection, Supervisory Control and Data Acquisition (SCADA) Cybersecurity, Developing Economies.

**Corresponding author: Ezirim Kelechi ThankGod*
Mechatronics Engineering Department; Federal University of Technology, Owerri, Imo State, Nigeria

Introduction

The integration of Information and Communication Technology (ICT) into power systems has spontaneously given rise to smart grids. In developing economies, smart grids are positioned as a solution to energy losses, load shedding, and grid instability (Amin & Wollenberg, 2005). However, this digitalization as noted by Stouffer et al. (2015), on the contrary expands the attack surface, particularly through Supervisory Control and Data Acquisition (SCADA) Control systems that monitor and control substations, transformers, and distribution networks. Tomanage this complexity relatively well, utilities are deploying ML-based IDS for real-time threat detection (Pan et al., 2019). While it appears effective against known attacks, ML models are also susceptible to Adversarial Machine Learning. Adversarial attacks introduce carefully crafted perturbations to sensor

data or network traffic in order to cause misclassification (Biggio & Roli, 2018). In SCADA environments, such misclassifications can lead to blackouts, equipment damage, or safety hazards (Cárdenas et al., 2008).

Admittedly, developing economies face peculiar and unique constraints ranging from aging infrastructure, intermittent connectivity to limited budgets for cybersecurity (Oyewole et al., 2021). These factors amplify SCADA vulnerabilities and hinder deployment of computationally expensive defenses.

Wang et al.(2022) pointed out that in spite of this temporary limitation, literature on Adversarial Machine Learning (AML) in smart grids has largely focused more on developed nations.

This paper addresses that gap by reviewing AML threat models, defense strategies, and SCADA-specific risks in developing economies with the aim to answer: What AML threats target smart grid IDS? Which defenses are feasible under resource constraints? What are the SCADA-specific gaps?

Literature Review

Smart Grid and Supervisory and Data Acquisition (SCADA) Security

SCADA systems form the operational backbone of smart grids, using protocols such as Modbus, DNP3, and IEC 60870-5-104 (East et al., 2009). These protocols were designed without security, making them prone to injection and replay attacks (Deng et al., 2011). In developing economies, legacy Remote Terminal Units (RTUs) and lack of patch management further increase exposure (Kuznetsov et al., 2020).

ML for Intrusion Detection

Supervised methods like Random Forest, Support Vector Machine (SVM) and Deep Neural Networks (DNN) are widely used for Intrusion Detection Systems (IDS) in smart grids (Zhang et al., 2017). Unsupervised and semi-supervised approaches address label scarcity (Li et al., 2018). However, model performance degrades under adversarial conditions (Szegedy et al., 2014).

Adversarial Machine Learning

Adversarial Machine Learning (AML) attacks are categorized as:

1. **Evasion:** Perturb test-time inputs to evade detection (Goodfellow et al., 2015).
2. **Poisoning:** Corrupt training data to degrade model performance (Barreno et al., 2010).
3. **Model Extraction:** Query the model to steal its architecture (Tramèr et al., 2016).

In smart grids, attackers target measurement data, network flows, and control commands (Erba & Tippenhauer, 2020).

Context of Developing Economies

Studies note that developing economies suffer from poor data curation, low redundancy, and limited incident response teams (Akinyele et al., 2022). This makes adversarial perturbations harder to detect and recover from.

Methodology

This review followed a structured synthesis approach. Searches from IEEE Xplore, ACM, ScienceDirect, and Scopus; Inclusion criteria of peer-reviewed papers between 2018-2025; Excluded papers without empirical evaluation or defense analysis and Extracted data on threat model, attack type, dataset, defense, and deployment context.

Results

Threat Models in Smart Grid Intrusion Detection Systems (IDS)

Threat Models in Smart Grid Intrusion Detection Systems (IDS) Evasion attacks are the most reported, often using FGSM and PGD to perturb PMU and SCADA traffic data (Chen et al., 2020; Yang et al., 2021). Poisoning attacks target training pipelines in utilities with weak data governance (Fawaz et al., 2022).

Defense Mechanisms

Common defenses include adversarial training (Madry et al., 2018), defensive distillation (Papernot et al., 2016), and anomaly detection with autoencoders (Zhang & Qi, 2019). However, adversarial training increases training cost by 3-5x, which is prohibitive for utilities in developing economies (Li & Vorobeychik, 2021).

SCADA-Specific Vulnerabilities

Three SCADA-specific issues emerged:

1. **Protocol Blindness:** ML models trained on TCP/IP data fail on DNP3 payloads (Vargas et al., 2019).
2. **Time-Criticality:** Defenses that add latency violate SCADA real-time requirements (≤100ms) (Amin et al., 2013).
3. **Data Scarcity:** Limited historical attack data in developing economies reduces robustness (Oyewole et al., 2021).

Deductions

From the synthesis, we deduce:

1. Adversarial Machine Learning (AML) risk is higher in developing economies due to legacy SCADA and low digital maturity.
2. Most existing defenses are not lightweight enough for field Remote Terminal Units (RTUs) and edge devices.

3. Protocol-aware feature engineering is underexplored but critical for SCADA.
4. Attackers can leverage knowledge of grid topology to craft more effective perturbations.

Discussion

The findings align with prior work on ICS security (Cárdenas et al., 2008) but extend beyond it to Adversarial Machine Learning. While developed nations can deploy ensemble defenses and cloud-based retraining, developing economies must rely on edge-compatible solutions.

A major conflict exists between detection accuracy and computational overhead. Adversarial training improves robustness but may be infeasible on devices with less than 2GB RAM (Wang et al., 2022). This suggests a need for transfer learning and federated approaches to share defense models across utilities without the risk of exposure in sharing raw data.

Furthermore, socio-technical factors matter. Limited cybersecurity workforce and vendor lock-in delay patching of SCADA vulnerabilities (Kuznetsov et al., 2020). Thus, technical defenses must be paired with policy to achieve maximum result.

Gaps and Future Targets

1. Lightweight Defenses: Research on quantized adversarial training and pruning for edge SCADA devices.
2. Protocol-Specific AML: Datasets and attacks modeled on IEC 61850 and DNP3.
3. Domain Adaptation: Models that transfer from simulated grids to real developing-economy grids.
4. Threat Intelligence Sharing: Regional ISACs for African and South Asian utilities.
5. Human-in-the-Loop: Interfaces to help operators interpret adversarial alerts.

Recommendations

For utilities and policymakers in developing economies:

1. **Adopt Tiered Defense:** Combine network Intrusion Detection Systems (IDS), host-based monitoring, and a robust adversarial ML at the control center level.
2. **SCADA Hardening:** Segment networks, disable unused protocols, and enforce authentication on RTUs (Stouffer et al., 2015).
3. **Capacity Building:** Train staff on AML and secure ML deployment.
4. **Public Datasets:** Fund creation of SCADA datasets reflecting developing economy grid conditions.
5. **Regulatory Mandates:** Require adversarial testing before IDS deployment in critical infrastructure.

Conclusion

Adversarial Machine Learning poses a credible threat to Machine Learning-based intrusion detection in smart grids. The risk is magnified in developing economies due to SCADA-specific vulnerabilities and resource constraints unlike in developed economies. Present defenses are largely designed for high-resource environments and do not translate directly. Future work should focus on lightweight, protocol-aware, and context-specific solutions. Securing smart grids in developing economies requires both technical innovation and institutional support.

References

1. Akinyele, D., Olabode, E., & Ajewole, T. (2022). Cybersecurity challenges in African power systems. International Journal of Electrical Power, 138, 107841.
2. Amin, M., & Wollenberg, B. (2005). Toward a smart grid. IEEE Power and Energy Magazine, 3(5), 34–41.
3. Amin, S., Cárdenas, A. A., & Sastry, S. S. (2013). Safe and secure networked control systems under denial-of-service attacks. IEEE Transactions on Automatic Control, 58(3), 563–576.
4. Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. Machine Learning, 81(2), 121–148.
5. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331.
6. Cárdenas, A. A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2008). Challenges for securing cyber physical systems. Workshop on Future Directions in Cyber-physical Systems Security, 1–7.
7. Chen, Y., Liu, S., & Zhang, Y. (2020). Adversarial attacks on deep learning-based power system state estimation. IEEE Transactions on Smart Grid, 11(4), 3465–3474.
8. Deng, R., Zhuang, P., & Liang, H. (2011). CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. IEEE Transactions on Smart Grid, 2(4), 724–735.
9. East, S., Butts, J., Papa, M., & Shenoi, S. (2009). A taxonomy of attacks on the DNP3 protocol. Critical Infrastructure Protection III, 47–58.
10. Erba, A., & Tippenhauer, N. O. (2020). No such thing as a free packet: A practical evaluation of stealthy attacks on industrial control systems. ACSAC, 555–568.
11. Fawaz, N., Atienza, D., & Giannakis, G. B. (2022). Data poisoning attacks on smart grid load forecasting. IEEE Transactions on Information Forensics and Security, 17, 1202–1214.
12. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. ICLR.

13. Kuznetsov, V., Escamilla-Ambrosio, P. J., & Giannetsos, T. (2020). A review of cybersecurity challenges in smart grids in developing countries. Energies, 13(17), 4542.
14. Li, X., & Vorobeychik, Y. (2021). Adversarial machine learning for cyber-physical systems. Foundations and Trends in Machine Learning, 14(4), 329–425.
15. Li, Z., Qin, Z., Huang, K., Yang, X., & Ye, S. (2018). Intrusion detection of SCADA systems using semi-supervised learning. IEEE Access, 6, 37267–37276.
16. Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2018). Towards deep learning models resistant to adversarial attacks. ICLR.
17. Oyewole, O., Ogunwuyi, O., & Adeyemi, B. (2021). Cybersecurity readiness in Sub-Saharan African energy sector. Energy Policy, 156, 112439.
18. Pan, S., Morris, T., & Adhikari, U. (2019). Developing a hybrid intrusion detection system using data mining for power systems. IEEE Transactions on Smart Grid, 6(6), 3104–3113.
19. Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). Distillation as a defense to adversarial perturbations. IEEE S&P, 582–597.
20. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev 2). NIST.
21. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. ICLR.
22. Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing machine learning models via prediction APIs. USENIX Security, 601–618.
23. Vargas, J., Gutierrez, J., & Cárdenas, A. (2019). Adversarial examples in ICS network traffic. Workshop on Cyber-Physical Systems Security, 25–32.
24. Wang, Y., Yang, Q., & An, D. (2022). A survey on adversarial attacks and defenses in smart grid. IEEE Communications Surveys & Tutorials, 24(2), 1210–1234.
25. Yang, Q., An, D., Min, R., Yu, W., Yang, X., & Zhao, W. (2021). On adversarial attack to deep learning-based intrusion detection for smart grid. IEEE Access, 9, 42588–42600.
26. Zhang, M., & Qi, H. (2019). Anomaly detection using autoencoders for SCADA systems. Applied Sciences, 9(21), 4653.
27. Zhang, Y., Wang, S., & Yohe, B. (2017). Machine learning based intrusion detection for smart grid. IEEE Transactions on Smart Grid, 8(4), 1680–1691.