IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

Guarding the Grid: Exploring Advanced Strategies for Detecting Intrusions in Power Distribution Devices

Sony Venugopal, Dr. Hannah Jessie Rani. R, Roopa. K.R

Research Scholar, Jain Deemed-to-be-University, Faculty, RNS Institute of Technology, Bengaluru, Karnataka, India

Assistant Professor, Jain Deemed-to-be-University, Bengaluru, Karnataka, India

Assistant Professor, Department of ECE, RNS Institute of Technology, Bengaluru, Karnataka, India

ABSTRACT: The modern power grid commonly referred to as the Smart Grid (SG), faces escalating cybersecurity concerns due to its intricate interconnections. As the backbone of energy distribution, power distribution devices are critical components vulnerable to anomalies and deliberate attacks. In this comprehensive review paper, we delve into advanced strategies for detecting intrusions within these devices. Our analysis encompasses existing approaches, highlighting their strengths and limitations. Additionally, we propose future research directions aimed at bolstering the resilience of power distribution systems, ensuring uninterrupted energy supply, and fortifying the security posture of the Smart Grid.

KEYWORDS: Intrusion Detection system (IDS), Smart Grid (SG), False Data Injection Attack (FDI), Artificial Neural Network (ANN).

I. INTRODUCTION

The SG combines communication, networking, and intelligence to efficiently allocate power resources. However, this interconnectedness introduces security risks, making the safe and stable functioning of power systems vulnerable to cyber attacks. These attacks compromise confidentiality, integrity, and availability (CIA) standards, threatening the entire energy infrastructure [1]. A SG is an enhancement of the traditional electrical grid, integrating two-way communications and distributed intelligent devices [7].It uses automation, communication, and IT systems to monitor power flows from points of generation to points of consumption, even down to the appliance level [8]. This allows the grid to control power flow or curtail the load to match generation in real time or near real time [8].

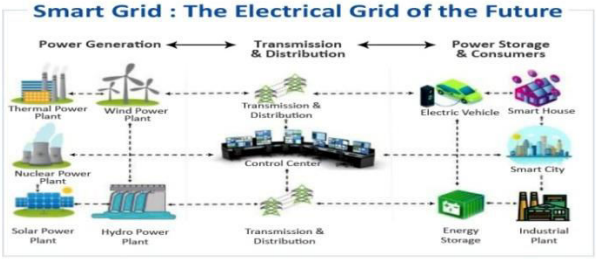

Fig 1.1 Typical SG structure

SGs contribute to the identification of losses and enable appropriate technical .and managerial actions to arrest these losses [8]. They can monitor, measure, and regulate power flows in real time, contributing to the reduction of transmission and distribution losses, peak load management, improved quality of service, increased reliability, better asset management, renewable integration, better accessibility to electricity, and the creation of self-healing grids [8].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

II. RELATED WORK

2.1Electric power systems overview

An electric power system is a huge set-up that connects power plants to end-users via an electric grid. Here are the key components of such a system:

Power Generation: Power plants convert various energy sources (such as coal, oil, natural gas, or renewable energies like water, wind, and solar) into electric energy. Conventional generators produce electricity at a frequency that is a multiple of the machine's rotation speed, typically ranging from 6 to 40 kV [11].

Transmission: The transmission network moves power from one part of a country or region to another. It consists of well-interconnected infrastructure with multiple power lines linking different substations. These substations change voltage levels, providing enhanced redundancy.

Distribution: Distribution networks deliver power locally to end-users (residential, commercial, or industrial).They act as the veins and arteries of our energy system, branching out from substations to homes and businesses. Key components include transformers, substations, and transmission lines, which work together to ensure a stable supply of electricity [12][13].

Cyber security Threats: As power distribution devices become more interrelated through smart grids, they are open to to cyber attacks. Intruders may attempt to manipulate control systems, disrupt communication networks, or compromise data integrity. Ensuring robust cyber security measures is vital to protect against such threats.

2.2 Effect of Cyber Attacks on SG

Cyber attacks can have severe disruptive effects on smart grids, leading to unsatisfactory behaviour, mal-operation of computers and electronic controls, tripping of motors and generators, load shedding, and cascading failure of the system [9]. These attacks can cause a .variety of severe consequences in the SG, from energy theft to massive blackouts or destruction to critical infrastructures [9].

One specific type of cyber attack is the FDI attack, which can cause the command and control center to give incorrect operational settings to the grid [10]. The impacts of this incorrect operational setting on the dynamics of the grid can be theoretically analyzed, and it has been shown that the FDI could potentially cause cascading failures due to possible overcurrent and voltage collapse [10].In this paper; we spotlight on the different strategies for guarding power distribution devices within the SG.

2.3 Vulnerable Power Distribution Devices

Smart grids, while enabling efficient energy management, also face cyber security threats due to their increased reliance on digital technologies. Critical Components vulnerable to cyber attacks in SG is sensors and actuators devices which play a essential role in monitoring and controlling grid operations. If compromised, they can disrupt grid functionality. RTUs collect data from the field devices and transmit it to the central control system. Attackers can target RTUs to manipulate data or disrupt communication. PLCs automate processes in the substations and distribution networks. Illegal access to PLCs can lead to grid instability. IT equipment used in SGs, such as switches and computers, are also vulnerable. Compromised switches can disrupt communication, and compromised computers can lead to illegal access [22]. The common attacks that affect SGs are Denial-of-Service (DoS) Attacks which overload grid components, causing service disruptions. In Phishing and Social Engineering, attackers scam users into revealing sensitive information or installing malicious software. Malicious actions by workers or contractor come under insider threats. Through malware attacks software is designed to harm or gain unauthorized access. The physical components are tampered with in physical attacks. Therefore the major consequences of cyber attack on SGs are service disruptions, data manipulation, financial losses, safety risks, reputation damage

III. METHODOLOGY

Traditional IDS have been used for network protection for decades. IDSs help protect against cyber threats by detecting and responding to suspicious activities.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

3.1 Signature-based Detection: These are a type of IDS that use predefined patterns or signatures to identify known types of cyber threats. These systems maintain a database of recognized attack signatures, which are pattern, associated with well-known attacks such as network scans, malware, or specific exploit attempts.

When set-up traffic passes through the IDS, it compares the observed patterns against the signatures in its database. If it finds a match, either exact or partial (for instance, specific byte sequences in packets or network flows), it triggers the detection process and raises an alert. Signature-based IDS are continuously active, analysing packets as they navigate through network. They can function at various points .within the network structure, including at the perimeter (like firewalls) or within internal network segments. The process of signature matching is comparatively simple, enabling signature-based IDS to swiftly identify known threats. They are.particularly effective at detecting attacks for which The algorithm automatically generates mask image without user interaction that contains only text regions to be inpainted. signatures already exist in their database. However, the primary drawback of signature-based IDS is their dependence on known signatures. They are .only capable of detecting attacks that .have been previously discovered and added to .their signature database. Consequently, signature-based IDS struggle to quickly adapt to new attack patterns, limiting their effectiveness against novel threats. That is the reason why they are. often used in conjunction with other types of IDS, such as anomaly-based or behaviour-based IDS, to provide a more broad defence against a wider range of threats. [1]

3.2 Anomaly-based IDS (ADS) play a major role in identifying deviations from normal behaviour within complex and dynamic systems like power grid. It focuses on identifying events or observations that appear doubtful when compared to expected or normal behaviour of the system. Unlike signature-based IDS that rely on predefined attack patterns, anomaly-based IDS use unsupervised learning techniques. They learn from old data without explicit labels for normal or anomalous instances. The IDS builds a model of that constitutes normal behaviour based on past data. This model captures statistical patterns, trends, and dependency within the system. During real-time monitoring, the IDS compare incoming data (e.g., sensor readings, network traffic) to the conventional model. If the. observed behaviour deviates significantly from the expected norms, the IDS trigger an alarm. Anomaly-based IDS can adapt to changes over time. As the system evolves or faces new conditions, the model adjusts accordingly. This adaptability is crucial for handling dynamic environments [15]. Power grids consist of numerous interconnected components—generators, transformers, transmission lines, substations, and distribution networks. Defining normal behaviour across this intricate web of dependencies is challenging. Power demand fluctuates throughout the day and across seasons. What's normal during peak hours may differ considerably from night-time behaviour. Anomaly detection models must account for these variations.

Anomaly-based IDS struggle with novel attacks or zero-day vulnerabilities. If an attack introduces previously unseen behaviour, the IDS may not recognize it as anomalous until it's too late. Anomalies are rare events compared to normal behaviour. Imbalanced datasets can lead to false positives or negatives. Ensuring sufficient representation of both normal and anomalous instances is essential. Power grid sensors may produce noisy or erroneous readings due to environmental factors or technical issues. Separating true anomalies from sensor noise is a challenge. Power grid topology changes due to maintenance, repairs, or load adjustments. Anomaly detection models must handle topology variations while maintaining accuracy. Operator errors, misconfigurations, or intentional actions (e.g., load shedding) can cause deviations from normal behaviour. Distinguishing between malicious and benign anomalies is critical. Intrusion detection plays a very important role in safeguarding the security and dependability of smart grids. Various strategies and methodologies have been implemented to detect intrusions in these systems. Furthermore, novel techniques and technologies are constantly emerging as the field progresses. Few prevalent methods and techniques employed for detecting intrusions in SG are mentioned below.

1. In the field of smart grid intrusion detection, several machine learning algorithms—such as decision trees, random forests, SVMs, and KNN—have been effectively used. These algorithms analyze network data to detect suspicious activities.
2. To detect intrusions in smart grids, deep learning technologies like CNNs, RNNs, and autoencoders are used due to their ability to capture complex data patterns.
3. Behaviour-Based Detection constructs a model based on expected actions from different components of the smart grid, including energy usage patterns. When inconsistencies are detected, the system generates notifications promptly.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

4. Attack graph-based detection involves using attack graphs to model attack sequences and vulnerabilities in the smart grid. Analyzing these graphs allows accurate detection of ongoing or planned attacks.
5. Monitoring and analyzing network traffic for unusual or malicious patterns is a common technique in network traffic analysis. This approach may include using network IDS and deep packet inspection (DPI) techniques.
6. Fuzzy Logic-Based Detection in smart grid systems creates models capable of representing uncertainties and imprecision using fuzzy logic. This makes it possible to carry out a more resilient ID. The execution of Hybrid Methods, which entail the combination of various detection techniques including signature-based and anomaly-based detection, may significantly enhance the precision and performance of intrusion detection systems.

IV. EXPERIMENTAL RESULTS

Valuating intrusion detection methods in smart grids involves finding out their performance using various metrics. The key metrics commonly used for this purpose:

1. Accuracy (ACC): This parameter finds out how well the intrusion detection system (IDS) correctly identifies attacks (true positives) and non-attacks (true negatives). It's usually expressed as a percentage or a ratio.

$$ACC=\frac{\text{True Positives+True Negatives}}{\text{Total Instances}}$$

2. Precision (PR): Precision (also called positive predictive value) is the ratio of true positives to the total number of positive predictions. High precision means fewer false alarms.

$$PR=\frac{\text{True Positives}}{\text{True Positives+False Positives}}$$

3. Recall (RE): Recall (or sensitivity) is ratio of true positives to the .total number of the actual attacks. It measures the system's ability to detect attacks. This measures the proportion of true .positive predictions among all actual positive instances.

$$RE=\frac{\text{True Positives}}{\text{True Positives+False Negatives}}$$

4. F1-Score: The F1 score combines precision and recall into a single metric. It balances false positives and false negatives.

$$\text{F1-Score}=2\frac{PR\cdot RE}{PR+RE}$$

5. Area Under .the Receiver Operating Characteristic Curve (AUC-ROC): Measures the model's capability to differentiate between positive and negative instances. AUC-ROC ranges from 0.5 (random guessing) to 1 (perfect classification).Higher AUC-ROC indicates better performance.

6. False Positive Rate (FPR): Measures the proportion of .false positive predictions among all actual negative instances.

$$FPR=\frac{\text{False Positives}}{\text{False Positives+True Negatives}}$$

7. False Negative Rate (FNR): Measures the proportion of false negative predictions among all actual positive instances.

$$FNR=\frac{\text{False negatives}}{\text{False Negatives+True Positives}}$$

8. Specificity (SPC): Also known as true negative rate. It measures the proportion of true negative predictions among all real negative instances.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

SPC=1−FPR

Author & Paper	Advanced Method Used	Advantages	Limitations	Types of Attacks Detected	Performance Metrics Evaluated
A. Aljohani et al[19]	Deep Learning neural network	High efficiency	Requires a real dataset for training. Computational complexity.	False Data Injection attack	Accuracy and Speed
Mitchell and Chen[17]	Machine Learning (ML)based IDS	Wide range of applications in transmission and distribution components. Insights into dataset generation and usage. Complexity analysis.	Specific ML algorithms may have limitations. Evaluation testbeds need to be carefully designed.	Insider attacks Malware propagation Data integrity violations	Execution Time Resource Utilization Scalability Robustness
Tariq, N et al[2]	Particle Swarm Algorithm combined with Random Forest	Distributed across WAN, HAN, and BAN in the smart grid.- Ensures information security.	Specific to Advanced Metering Infrastructure (AMI). May require fine-tuning for different grid architectures.	Cyber attacks on smart meters Unauthorized access	Detection Accuracy FPR FNR Precision Recall F1 Score
Mehdi Jabbari Zideh[22]	Autoencoder and GAN	Superior Performance Utilization of GAN Model Integration of LSTM	Requires a longer training time compared to other supervised and unsupervised models due to the embedded Generative Adversarial Network (GAN) and Autoencoder (AE) components	False data injection attacks	Accuracy Precision Recall F1 Score
Tariq et al[2]	Fog-edge-enabled IDS	Utilizes fog computing for intrusion detection. Addresses real-time threats in smart grids.	Specific to fog-edge architecture. May need adaptation for different grid scales.	Data manipulation attacks - Energy theft	Detection Accuracy FPR FNR Precision Recall F1 Score
Jokar et al[4]	Model-based IDS for Home Area Networks (HAN)	Considers neural networks, genetic algorithms, and decision trees. Suitable for HAN security.	Specific to HAN context. May not cover entire smart grid.	Unauthorized device access - Data integrity violations	Execution Time Resource Utilization Scalability Robustness

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

Zhang et al[21]	Convolutional Neural Network (CNN) combined with Gated Recurrent Unit (GRU) and Fuzzy Logic (FL)	- Real-time intrusion detection in smart grid environments. - Improved accuracy using deep learning techniques.	- Requires labeled training data. - Computational complexity.	- Network security intrusions	- Detection Accuracy - False Alarm Rate - Precision - Recall

V. CONCLUSION

In conclusion, the cyber security landscape of power grids is evolving rapidly, and the call for advanced intrusion detection strategies is more critical than ever. This research has explored various approaches to detecting intrusions in power distribution devices, each with its distinctive strengths and challenges. Machine learning-based methods have shown promise due to their ability to learn and adapt to new threats. However, they require .huge amounts of .data for training and may struggle with zero-day attacks. Rule-based systems, on the other .hand, are excellent at detecting known threats but may fail to identify novel attacks. Hybrid systems that combine the strengths of ML and rule-based approaches could potentially offer a more robust solution. However, developing such systems poses significant challenges, particularly in terms of integration and scalability. Furthermore, the increasing interconnectivity of power grids, while beneficial in many ways, also opens up new avenue for cyber attacks. Therefore, future research should focus on developing intrusion detection strategy .that can effectively handle the difficulty and scale of interconnected power grids. Finally, it is vital to stay in .mind that technology alone cannot fully secure power grids. A broad approach that includes policy measures, regular audits, employee training, and public awareness is necessary to guard the grid effectively.

REFERENCES

[1] Dasgupta, R., Pramanik, M., Mitra, P., & Roy Chowdhury, D. (2024). Intrusion detection for power grid: a review. International Journal of Information Security, 23, 1317–1329.
[2] Tariq, N., Alsirhani, A., Humayun, M., Alserhani, F., & Shaheen, M. (2024). A fog-edge-enabled .intrusion detection system for smart grids. Journal .of Cloud Computing, 13(43).
[3] Krause, O., & Böhm, K. (2021). Classifying resilience approaches for protecting smart grids against cyber attacks. International Journal of Information Security, 23, 1317–1329.
[4] Jokar, P., & Dehghantanha, A. (2022). Machine Learning-based .Intrusion Detection for Smart Grid Computing. *ACM
[5] Kumar, A., Bhushan, B., Nand, P. (2022). Preventing and Detecting Intrusion of Cyber attacks. in Smart Grid by Integrating Blockchain. In: Sharma, D.K., Peng, SL., Sharma, R., Zaitsev, D.A. (eds) Micro-Electronics and Telecommunication Engineering . ICMETE 2021. Lecture Notes in .Networks and Systems, vol 373. Springer, Singapore. https://doi.org/10.1007/978-981-16-8721-1_12
[6] Smart Grid - Wikipedia
[7] National Smart .Grid Mission, Ministry of .Power, Government of India
[8] Olowu, T.O., Dharmasena, S., Hernandez, A., Sarwat, A. (2021). Impact Analysis of Cyber Attacks on Smart Grid: A Review and Case Study. In: Tyagi, H., Chakraborty, P.R., Powar, S., Agarwal, A.K. (eds) New Research Directions in Solar Energy Technologies. Energy, Environment, and Sustainability. Springer, Singapore. https://doi.org/10.1007/978-981-16-0594-9_3
[9] B.M. Ruhul Amin, Seyedfoad Taghizadeh, Md. Shihanur Rahman, Md. Jahangir Hossain, Vijay Varadharajan, Zhiyong Chen,First published: 02 October 2020, https://doi.org/10.1049/iet-cps.2019.0103
[10] https://electrical-engineering-portal.com/electric-power-systems
[11] https://www.electricityforum.com/td/overhead-td/power-distribution
[12] https://www.graygroupintl.com/blog/energy-infrastructure
[13] https://www.energy.gov/sites/default/files/2023-11/FINAL_CESER%20Electricity%20Grid%20Backgrounder_508.pdf

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308103|

[14] Madabhushi, S., & Dewri, R. (2023). "A survey of anomaly detection methods for power grids." International Journal of Information Security, 22, 1799–1832

[15] Zhao, H., Liu, G., Sun, H., Zhong, G., Pang, S., Qiao, S., & Lv, Z. (2023). An enhanced .intrusion detection method for AIM of smart .grid. Journal of Ambient Intelligence and Humanized Computing, 14(2023), 4827–4839

[16] Yu, T., Da, K., Wang, Z., Ling, Y., Li, X., Bin, D., & Yang, C. (2022). An Advanced .Accurate Intrusion Detection System for Smart Grid Cyber security Based on Evolving Machine Learning. Frontiers in Energy Research, 10, 903370. doi: 10.3389/fenrg.2022.903370

[17] Mitchell, R., & Chen, Y. (2021). A .Comprehensive Review on Cyber-Attack Detection and Control of Micro grid Systems. In Cyber Kill Chain-Based Hybrid Intrusion Detection .System for Smart Grid .

[18] Ghiasi, Mohammad & Dehghani, Moslem & Niknam, Taher & Kavousi-Fard, Abdollah. (2020). Investigating Overall Structure of Cyber-Attacks on Smart-Grid Control Systems to Improve Cyber Resilience in Power System.

[19] A. Aljohani, M. AlMuhaini, H. Poor and H. Binqadhi, "A Deep Learning-Based Cyber Intrusion Detection and Mitigation System for Smart Grids" in IEEE Transactions on Artificial Intelligence, vol. 1, no. 01, pp. 1-13, 5555.doi: 10.1109/TAI.2024.3354688

[20] Li, Y., Ji, X., Li, C., Xu, X., Yan, W., Yan, X., Chen, Y., Xu, W.: Cross-domain anomaly detection for power industrial control system. In: 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 383– 386. IEEE (2020)

[21] Zhang, Y., Wang, L., Sun, W., Green, R.C., II., Alam, M.: Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans. Smart Grid 2(4), 796 (2011)

[22] Mehdi Jabbari Zideh, Mohammad Reza Khalghani, Sarika Khushalani Solanki,
An unsupervised adversarial auto encoder for cyber attack detection in power distribution grids, Electric Power Systems Research, Volume 232, 2024, 110407, ISSN 0378-7796,https://doi.org/10.1016/j.epsr.2024.110407

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details