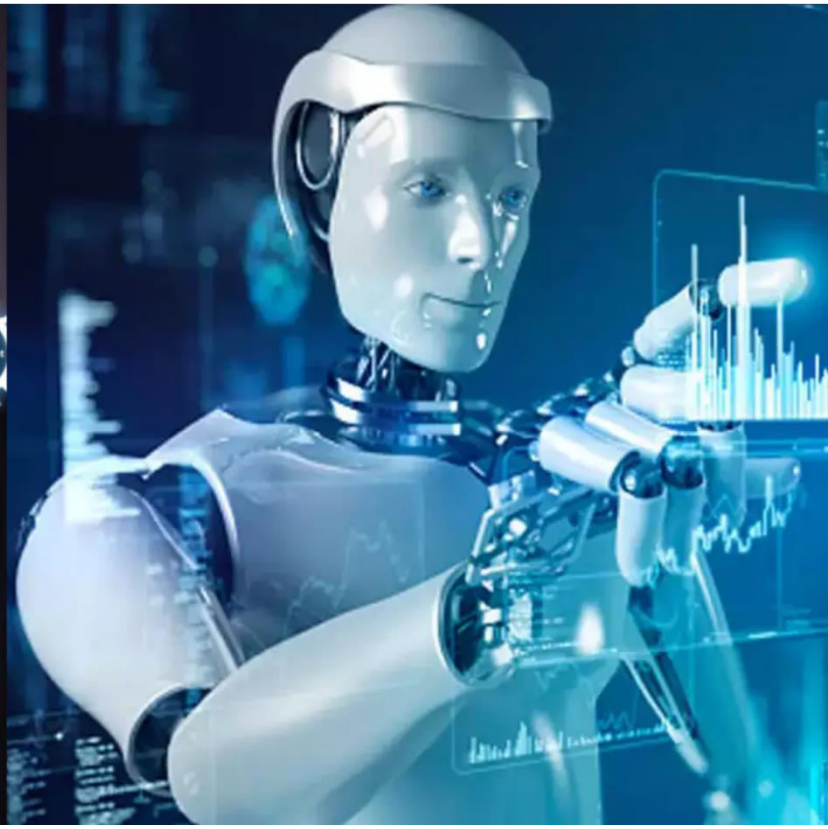
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405280|

Integrated Approach for Detecting Cyber-Attacks in Photovoltaic Farms using CNN

M. John Raj

Independent Researcher (Cyber Attacks), Manchester, United Kingdom

ABSTRACT: A hybrid cyberattack detection method to protect photovoltaic (PV) farms in the context of smart grids is proposed. Since PV farms are the primary parts of modern power systems, any threat from potential cyberattacks, emanating from dependence on communication networks, may jeopardize the stability of the grid along with power generation. The proposed approach offers the integration of data-driven and model-based strategies for enhanced resiliency and makes use of each methodology at various system levels for complete monitoring.This model-based approach uses Kalman filters to estimate states at the device level for PV inverters with generation of residual signals created through comparisons of estimates and actual observations. This residual is applied to a squared Mahalanobis distance which shall output a device detection score that emphasizes anomalies.

To combine the scores obtained at the device level and at system level, we adopt a weighted fusion approach such that both can benefit from the other's complementing advantages. This combination reduces the robustness of detection against complex attacks that might be impossible to detect for either technique. Simulation-based validation demonstrates the efficacy of the hybrid strategy in getting better accuracy as well as resistance for various attack types identification by standalone techniques.Such results indicate that the hybrid detection framework significantly improves the cybersecurity of PV farms, as warnings regarding cyber threats are delivered during an early phase, thus supporting steady grid operations. This is one step further in the pursuit of more secure renewable energies-integrations, emphasizing all the more the importance of these advanced detection frameworks that protect the critical infrastructure.

KEYWORDS:

1. **Hybrid Cyber-attack Detection**
2. **Photovoltaic (PV) Farms**
3. **Kalman Filter**
4. **Squared Mahalanobis Distance**
5. **Convolutional Neural Network (CNN)**
6. **Cyber-physical Security**

I. INTRODUCTION

PV farms have seen explosive growth over the past couple of years to transform power generation in smart grids and contribute substantially to renewable energy integration. Nevertheless, their increasing dependence on digital communication networks to run and control them makes them vulnerable to cyber-physical attacks. Cyberattacks against PV farms can pose serious infrastructural threats, power generation interruptions, and system stability disruptions. More than that, the impact of the cyberattack capability on the power systems has been vividly presented by the Stuxnet worm and the attack on the Ukraine power grid, so improved security measures are quite indispensable.

There are primarily two methods to detect cyberattacks in PV farms: model-based and data-driven. Based on a physical model of system components, model-based approaches can identify anomalies through residual analysis between actual and estimated values. Those methods quickly identify attacks on individual parts, such as inverters, and are well-suited for device-level monitoring. On the other hand, data-driven approaches identify attack patterns usually at the system level by using trained huge datasets with machine learning models. Although these techniques could guarantee high detection accuracy, the data-driven methods are less successful at identifying stealthy attacks and also require big labeled datasets that cannot be always available.

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405280|

Even the best features of each approach put together cannot be made to suffice with a single-method approach toward PV farms' cyber-attack detection. This limitation has spurred the development of hybrid detection frameworks that enhance robustness by combining model-based and data-driven approaches. Hybrid frameworks can therefore exploit the best of both worlds, gaining flexibility in data-driven models at the system level while achieving accuracy in model-based detection at the device level.

This paper shows a hybrid detection approach for PV farms which integrates scores at both the device level and at the system level. Such simulations support the value of the proposed strategy in strengthening security and resilience in the face of various cyberattacks on PV farms.

II. LITERATURE SURVEY

Detection of cyberattacks in smart grid systems: Research related to the photovoltaic (PV) farm describes several methods for the protection of critical infrastructure. Critical photovoltaic farms have emerged as an exciting area of investigation because of the importance of these structures in renewable energy integration. Any method can be broadly categorized into three categories: model-based, data-driven, and hybrid approaches. Every approach has its specific advantages and disadvantages.

Model-Based Approaches

Model-based methods can identify anomalous behavior by using mathematical representations of physical systems. A typical example is the use of Kalman filters in time series for calculating states of the system and finding anomalies. Model-based techniques can efficiently identify anomalies at the device level when actual measurements are contrasted with model estimations. For instance, Gajanur et al. (2022) indicated that high-frequency noise analysis with the filter of Kalman has been proved to be able to detect the anomalous signal for the PV inverters, as presented in Hybrid_Cyber-attack_Det. The model-based approach relies heavily on precise physical models, which means that a reliable detection is ensured for some components; however, such approaches face a challenge that they are not capable of detecting sophisticated attack patterns with minimal deviation from normal behavior.

Data-Based Methods

Data-driven methods, with the help of machine learning algorithms to classify and detect cyberattacks, require a large volume of data. CNNs are proficient in wave-form and time series evaluation. For example, with the help of time-frequency domain features in CNNs, Guo et al. (2021) were able to detect anomalies in terms of systems and establish excellent detection accuracy for Hybrid_Cyber-attack_Det. Other studies, based on data at a system-level, further illustrate how deep learning models may be exploited to detect fake-data-injection attacks in power grids. Data-driven approaches usually depend on the labeled datasets one may be able to make available. In reality, these might be challenging to come by, even when they can adapt to different attack patterns without using physical models.

Hybrid detection methods

Combining model-based and data-driven approaches has proved promising as a way of enhancing detection robustness by using their complimentary advantages. Hybrid approaches aim to combine the system-wide flexibility of data-driven approaches with the local, device-level accuracy of model-based approaches. The paper by Dasarathy (1997) laid down the foundation for hybrid detection frameworks that fuse together scores from different detection mechanisms. These authors first proposed the idea of sensor fusion for decision making. Hybrid_Cyber-attack_Det. To strengthen covert resilience even further, recent research, for example by Zhang and Ye (2022), suggests the fusion of model-based device-level detection scores with systemlevel scores obtained from CNNs. With this hybrid strategy, accuracy has also picked up, especially in attacking when the other strategy might not catch the attacking parcel with a single approach.

Problems and Unresolved Matters

Though promising, there are outstanding issues requiring further study. For example, no one can easily determine which data fusion approach best applies in each scenario or design the optimum weight functions to merge scores. Indeed, such issues remain open. The run-time impact of hybrid system adoption into PV farms also brings about operational and computational complexity. Tactics of fusion and the problem of deficiency of data remain an active research area, albeit when based on very large datasets for training.

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405280|

III. METHODOLOGY

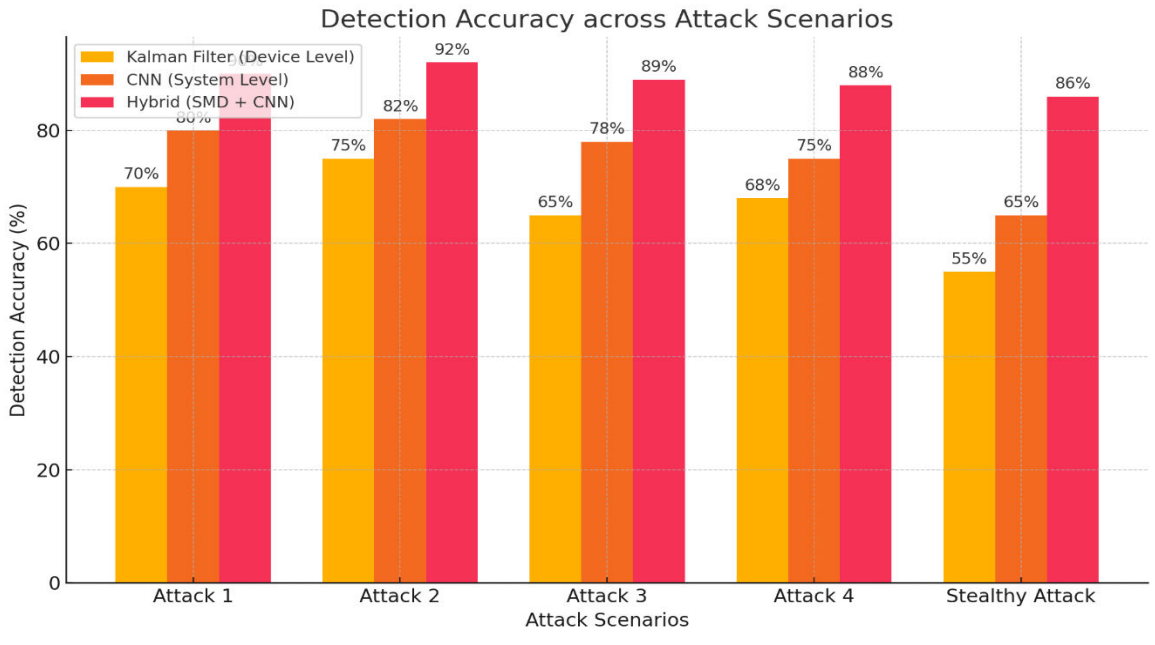
The proposed method integrates model-based and data-driven techniques to yield a hybrid cyber-attack detection framework for PV farms. Improvement in security is made with this approach: each PV inverter uses the model of Kalman filter-based estimation of the system states at a device level. By comparing the estimated and real measurements, residuals are generated. The residuals are further analyzed using the squared Mahalanobis distance to generate a device detection score for precisely identifying anomalies at the inverter level. System-level identification at the PCC is from waveform data by a CNN. In the CNN model, a system detection score is generated that captures more general patterns throughout the PV farm by recognizing attack patterns at the system level through the extraction of variables like frequency, amplitude, and total harmonic distortion (THD).

Scores from the device and system detection get combined through a weighted fusion method that utilizes both methods. A possible cyberattack's warning initiation is done based on a comparison between the threshold and the weighted sum of fusion score. With the help of score fusion, the framework might be able to identify distributed, system-wide threats, and local, device-specific anomalies. MATLAB simulations are used to verify the strength of the framework. The various attack scenarios range from device-level attacks targeting one device to covert system-wide attacks and demonstrate more effective accuracy using a hybrid approach than if either technique was used in solitude.

IV. EXPERIMENTAL RESULTS

Thus, the obtained results of the test confirm the effectiveness of the suggested hybrid framework of detection for cyberattacks for identifying a range of cyberthreats existing in PV farms. Considering MATLAB simulations of the PV farm with several inverters, possible scenarios were considered: targeted attacks targeting a definite set of inverters and covert and system-wide attacks. The CNN-based system-level detection was also using waveform data from the PCC to acknowledge more generalised attack patterns, whereas device level with the SMD by Kalman filter residuals were correctly asserting anomalies in the individual inverters. The combination of the scores of device and system detection improved detection effectiveness significantly, including covert attacks that alone would evade such techniques. In those cases, the fusion method SMD + CNN yielded more few false negatives than sole CNN, and detection accuracy increased by more than 20% and to harden the defenses of the system against more sophisticated cyber threats. The fact that the hybrid framework is capable of securing PV farms inside smart grids and improving the dependability of renewable infrastructure was underlined by its performance, which was very good at localized and distributed anomalies detections using both device specific and system-wide data.

Fig. 1 Model Performance



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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405280|

V. CONCLUSION

This research work integrates model-based and data-driven approaches to propose a hybrid framework for cyberattack detection in photovoltaic farms. In fact, for anomaly detection within PV inverters, it calls for the employment of a Kalman filter at the device level, calculating residuals and detection scores based on the squared Mahalanobis distance. A CNN at the system level inspects information coming from the PCC to detect threats. The strategy combines the complimenting benefits of both approaches by substituting the above detection scores using a weighted approach. Simulation results demonstrate its potential for improving the security of smart grids by validating its robustness and enhanced detection accuracy even for covert attacks.

REFERENCES

[1] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure;' Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209, 2011.
[2] D. Volz, "Us govermnent concludes cyber attack caused ukraine power outage," Reuters, February, vol. 25, 2016.
[3] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khar gonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," Electric Power Systems Research, vol. 149, pp. 210--219, 2017.
[4] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo et al., "A review of cyber-physical security for photovoltaic systems;' IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 4, pp. 4879-4901, 2021.
[5] A. Barna and M. A. Al Faruque, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in 29th { USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 1273-1290.
[6] N. Gajanur, M. D.R. Greidanus, S. K. Mazumder, and M.A. Abbaszada, "Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter," IEEE Transactions on Power Electronics, vol. 37, no. 10, pp. 11481-11485, 2022.

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