Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Powered Anomaly Detection in Solar SCADA Systems: Challenges and Solutions

Priyanka Ashfin
Independent Researcher, Eden Mahila College, Bangladesh
Corresponding Author: Priyanka Ashfin**, E-mail**: *priyanka.ashfinn@gmail.com*

| ABSTRACT

The digital transformation of solar energy environments has left them exposed to cyber and operational threats, especially in SCADA systems that control photovoltaic (PV) plants. Conventional rules-based monitoring solutions are becoming inadequate to manage how large, complex and real-time the smart grid has become. In this paper, an AI-based anomaly detection framework using deep learning models (CNN and LSTM) is proposed to detect abnormal patterns in solar SCADA data streams. Both process variables (e.g., voltage, current, irradiance, inverter temperature) and network traffic metrics are considered by the proposed system while querying false data injection, DoS attack and communication-layer anomalies. Experimental subject results obtained on hybrid real-time datasets prove that the proposed model attains more than 96% detection efficiency, substantial decrease in false alarm rate (FAR) and latency when compared to conventional machine learning classifiers. The framework further includes online adaptation that provides adaptive retraining capabilities for addressing concept drift due to environmental and operational changes. These results demonstrate that the AI-based anomaly detection capability not only improves cybersecurity of cyber-physical systems and the data integrity, but it also helps predictive based maintenance and operation robustness of PVs. Lastly, the paper reviews major hurdles (e.g., paucity of datasets, model explanation and edge deployment limitations) and proposes practical solutions to embed intelligent anomaly detection in nextgeneration secure-, autonomous- and sustainable-based solar SCADA ecosystems.

| KEYWORDS

Solar energy, SCADA systems, anomaly detection, deep learning, cybersecurity

| ARTICLE INFORMATION

ACCEPTED: 01 November 2022 **PUBLISHED:** 12 December 2022 **DOI:** 10.32996/fcsai.2022.1.1.2

1. Introduction

Solar photovoltaic (PV) technology has been rapidly growing and it is being considered as one of the most promising foundations for global energy transition. Based on these it was estimated by end of 2022 the globally installed solar capacity has exceeded 1,185 GW which experienced more than a 20 % year-on-year growth rate (Harrou et al.,). This increasing uptake owes much to the emergence of supervisory control and data acquisition (SCADA) systems allowing for remote operation, real time watching and data based fine tuning of PV sites. SCADA systems are the operational brains behind utility scale solar plants, which connect sensors, programmable logic controllers (PLCs) and networked gateways to capture data on performance parameters (voltage, current, irradiance, inverter temperature and energy yield) (Lee et al.,). However, these systems have become slowly less and less mechanical in nature, as they ecosystems are increasingly digitized and network-connected - adding a new layer complexity in both security as well as reliability-, with anomaly detection being a primary area of concern for modern solar operations.

Entire Solar Power Generation visibility Sense IoT allows monitoring of the end to end solar power generation, helping operators to take immediate action for optimisation and predictive maintenance. They gather measurements from a number of field devices through industrial communication protocols (e.g., Modbus, DNP3, or IEC 104) and transmit this data to centralized control centers or cloud-based dashboards (Lin et al.,). Such systems are necessary to adjust generation and demand, identify malfunctioning equipment, and maximize performance at multiple plants of widely varying sizes spread over wide areas.

Yet as PV installations are becoming more and more IoT-integrated with cloud connections and remote handling, SCADA environments become subject to network-borne cyber threats. Attackers may abuse flaws in communication protocols, authentication mechanisms, or software interfaces to tamper data of system/halt communication/disrupt control signals for the inverters (Harrou et al.,). These disturbances can lead to significant loss of energy, damage equipment, or cause grid instability.

The Evolving Threat Landscape of Solar SCADA Systems

The solar SCADA attack surface exploded with the dawn of Industry 4.0 and IIoT (Industrial Internet of Things) communications connectivity. Recent events in the energy domain have shown that the operational technology (OT) infrastructures are being threatened by means of injects of false data injection (FDI), denial-of-service (DoS), malicious entry points and fake command sequences (Pinto et al.,). For instance, tampering with inverter telemetry may lead to the control system over- or under-compensating for energy production, which can result in imbalances on the grid. Also, a simultaneous attack on gateway communication paths regarding DoS can interrupt data transfer to falsify faults or resist special treatments (Ahakonye et al.,).

Conventional signature-based or rule-based intrusion detection systems (IDSs)—which are effective at spotting known patterns often struggle to classify new, novel and zero-day attacks, particularly in dynamic scenarios affected by changing load situations and noisy sensor signals (Mohammadpour et al. Adding to the complexity of fixed-rule detection is the distinct operational variability of PV systems due to sunlight intensity, shading patterns, temperature, and equipment aging. These restrictions clearly illustrate the necessity for AI-based detection systems which can discover from complicated multi-dimensional, non-linear relations in data that are common to solar SCADA operations.

Next-generation solution: Anomaly detection and AI in 2020 As machines continue to be deployed into ever more complex environments – what I will refer to as machine complexity - the importance for this pattern-matching technology becomes irrefutable.

Artificial Intelligence (AI), especially machine learning (ML) and deep learning (DL), has been recognized as a disruptive approach in cyber-physical security and condition monitoring. AI models can detect faint signals of attacks or anomalies that indicate errors if they learn from data rather than using prewritten rules. of architectures), CNNs are well-suited for capturing the local spatial correlations between a set of variables in our case—voltage–current–power relationships while RNNs and LSTMs can capture sequential dependencies over time (Gyamfi et al., 2022). Hybrid architectures of CNN–LSTM networks, for example, are a strong combination to spot both instantaneous and evolving anomalies in SCADA streaming data (Ahakonye et al.,).

A number of researches have shown that these models are promising for energy and industrial applications. For instance, Lee et al. developed the packet level anomaly detection method for solar plant network by using deep learning and their proposed system obtained better accuracy than conventional IDS techniques. Similarly, Lin et al. proposed a hybrid-neural network-based intelligent Modbus anomaly detection approach, where the capabilities of them were emphasized in renewable energy communication links. These results cumulatively indicate that AI driven systems can be superior than classical ones in terms of accuracy and latency factors, which are critical for the operational security within SCADA-oriented PVs.

Issues with AI for Solar SCADA Security Deployments

Although AI has so many benefits, there are several challenges of using this technology in solar SCADA.

Data scarcity and imbalance: Live labeled cyber-attack event datasets are a small set, due to proprietary issues (which limit access) but also due to the fact that real intrusion data is very rare. Therefore, models based on generic IoT data can poorly generalize to solar specific patterns (Pinto et al.,).

Concept drift: Variations in the environment and seasons lead to changes in normal patterns over time which needs to constantly provision new models (Harrou et al.,).

Computational and latency issues Real-time detection requires: edge deployable models with low inference time and resource consumption (Al Nuaimi et al.,).

Interpretability and trust: Operators require explainable AI decisions to react in time with corrective actions. There is a risk that lack of explainability will be a barrier for adoption in critical infrastructure (Gyamfi et al., 2022).

Overcoming these challenges motivates a unified approach which combines data engineering, model tuning, and domain-specific contextualization of anomalies in PV operations.

Research Motivation and Objectives

Considering the drawbacks of traditional SCADA monitoring and AI technology revolution, we here propose to develop an AI based anomaly detection proposal for solar SCADA systems. The primary objectives are:

- To design a hybrid CNN–LSTM deep learning model for the online detection of cyber and operational anomalies in solar power time series.
- To compare it performance with that of classical ML classifiers by mean of accuracy, F1-score and alarm rates.
- To overcome the issues of implementation regarding data imbalance, complexity and concept drift.
- To present and demonstrate potential solutions to integrating AI-based security models into practical solar SCADA environments under acceptable cybersecurity frameworks like NIST IR 8228 (2019) and ISA/IEC 62443 (2021).

This work promotes the resilience and sustainability of REE by integrating intelligent cybersecurity features into the operational behavior of solar environments.

Structure of the Paper

The rest of this paper is organized as follows: Section 2 reviews related works about anomaly detection in PV and SCADA systems; Section 3 introduces the proposed AI technique of methodology, and system architecture specifics; Section 4 shows that experiments are conducted on real-world testbeds for performance evaluations, and discussions will be provided in Section 5 finds are discussed to highlight findings as well as implications and limitations, which is followed by conclusions with later work described in Future directions for AI-enhanced solar cybersecurity.

2. Literature Review

An AI-Based Anomaly Detection in Solar SCADA Systems: The Challenges and Solutions

SCADA Systems in Solar Energy: A Brief Introduction

For large-scale solar photovoltaic (PV) plants, the SCADA (Supervisory Control and Data Acquisition) system is their nerve center. They acquire raw data from sensors, inverters and controllers deployed within solar farms in real-time and then analyze and display it (Harrou et al.,). The SCADA system architecture generally includes field devices like RTUs, PLCs etc (e.g., Remote Terminal Units or Programmable Logic Controllers), communication networks with industrial protocols utilized (e.g., Modbus, DNP3, IEC 60870-5-104) and a centralized HMI. These systems are vital for regulating operational conditions such as DC voltage, current, light, inverter temperature and energy production (Lee et al.,).

But as solar grows larger and more sophisticated, SCADA is coming together with cloud-based IoT platforms so that you can monitor energy production remotely do predictive maintenance. This IT and OT merge, although enhancing operational quality, brings challenges to PV infrastructures including data compromise, unauthorized access and communication failures (Pinto et al.,). Therefore, the reliability and security of SCADA data streams is a significant issue that must be addressed in the management of renewable energy systems.

Cyber-Physical Threats and Anomalies in Solar SCADA Systems

The increasing adoption of renewable energy assets has broadened the attack surface for incidents targeting SCADA networks. Typical cyber attacks are false data injection (FDI), denial- of-service (DoS), malware attack, and replay attack (Harrou et al.,). Robustness of cyber attacks, in particular FDI can alter sensor or meter readings without being detected by standard validation alert will lead to incorrect control strategies. Studies by Liu et al. (2020) and Pinto et al. describe how such attacks can disrupt power forecast models and grid balancing algorithms for PV generation.

Communication channels are commonly attacked with DoS which disable proper exchange of data between the field equipment and control center by flooding communication links, – (Ahakonye et al.,,). Also, spoofing and replay attacks can impersonate valid devices or re-play old control commands that have been captured before in order to turn off inverters or manipulate voltage control logic (Lin et al.,). Traditional SCADA solutions depend on deterministic communication and fixed thresholds, so they usually cannot discover complex, slowly-changing, or stealthy anomalies in the operational data.

In addition, most PV systems do not have encryption, intrusion defense and authentication mechanisms as a result of obsolete hardware and real-time performance limitations (ISA/IEC 62443, 2021). Cyber incidents may, therefore, remain undetected until after substantial operational or monetary loss occurs. Dar...These attacks emphasize the necessity of security mechanisms that are adaptive, intelligent and self-learning such they can handle high-dimensional non-linearogen et al. flow data in real-time.

Machine Learning Based Anomaly Detection in SCADAframes, but without all of the features.

Machine Learning (ML) has shown its dominance in industrial anomaly detection in the past decade. Traditional ML techniques, like SVM, Decision Trees (DT), Random Forest (RF) or K-Nearest Neighbors (KNN), have demonstrated the capability to classify abnormal behaviors from process and network data. For example, Sreenu and Durai (2020) showed the performance of an SVM-based intrusion detection model has demonstrated 90% accuracy using an industrial IoT testbed. The traditional algorithms, however, leverage feature engineering and have limited temporal context in the training data, which diminishes their capability to identify novel or evolving attack vectors.

In solar SCADA, the data is temporal, multivariate and very dynamic due to environmental driven factors including irradiance, temperature and cloud cover. And therefore, models that are capable of learning rich, time-dependent patterns would be more appropriate. This has driven a trend from shallow ML toward DL methods (Mohammadpour et al., 2022).

Deep Learning for Anomaly Detection

The deep learning model could automatically learn hierarchical features from raw data without human-customized feature engineering. Several different DL architectures have been investigated for industrial and energy systems to perform anomaly detection:

- Autoencoders (AEs): Applied to unsupervised learning, where the model reconstructs input data and calculates reconstruction error as an anomaly score. Performance for distinguishing unseen attacks (Yao et al.,).
- Convolutional Neural Networks (CNNs): The networks used for capturing patterns and correlations among process variables or packets in network flow based on their spatial radiancy. CNNs have demonstrated promising results in DDoS and protocol intrusion detection (Mohammadpour et al., 2022).

- Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM): RNNs and LSTMs have been shown to work well with time-series data, they model temporal dependencies making them capable of early detection of a slow attack or equipment degradation (Ahakonye et al.,).
- Hybrid CNN–LSTM models, which factors in together the local spatial convolutional structure of CNN and the temporal sequence relationship modeling of LSTM to detect instantaneous and time-evolving anomalies. Hybrid approaches to detection have demonstrated above 95% accuracy in the study of smart grid cybersecurity (Pinto et al.,).

For example, Lee et al. trained a deep learning model for detecting anomalies in PV inverter communication packets with CNN, and the detection accuracy was more than 96%. Similarly, Lin et al. also introduced a hybrid CNN–GRU based on Modbus traffic anomaly detection which was more robust than the shallow ones. The findings in these studies demonstrate that the capability of deep learning can be leveraged to improve real-time anomaly detection on SCADA systems, particularly for high volume and velocity.

Issues in AI-Based SCADA Security for Solar

AI has huge potential, but there are a number of roadblocks to its adoption:

Dataset restrictions – The majority of public intrusion detection datasets (e.g., NSL-KDD, CIC-IDS2017) is not designed for solar or SCADA scenarios in particular(Pinto et al.,). The lack of labeled, domain-appropriate datasets is an obstacle to model generalization.

Class imbalance -Attack events are only a proportion of the entire operational data, and models tend to be biased as a result. Methods such as SMOTE oversampling and one-class learning have been suggested to address this (Gyamfi et al., 2022).

Concept drift – Environmental variation modifies the system's normal operating behavior, leading to performance degradation over time (Harrou et al.,). Active research on online and transfer learning are studying how to continually adapt.

Edge deployment and latency - AI models that are deployed on the edge need to work under low-latency and limited resources too. Lightweight model deployment to microcontrollers has become possible with the help of efficient frameworks such as TensorFlow Lite and ONNX (Al Nuaimi et al.,).

Model interpretability – Deep learning models are often referred to as "black boxes." The adoption of Explainable AI (XAI) tools like SHAP and LIME will improve the interpretability and drive operators trust towards it (Gyamfi et al., 2022).

Solutions and Emerging Trends

Based on the recent literature, hybrid and adaptive AI architecture will form the future for SCADA anomaly detection in solar system. Several key strategies have emerged:

- Federated learning: Enables collaborative training among the distributed PV sites without transferring data to a central place, thus enhancing the privacy and adaptability.
- Transfer learning: Adopts pre-trained models on generic industrial datasets and fine-tunes them under specific solar conditions.
- Edge intelligence: Deploys compressed AI models at the device or at a gateway to enable near-real-time detection (Kong et al., 2022).
- Cybersecurity framework integration: Such AI detection can be harmonized with the NIST IR 8228 (2019) and ISA/IEC 62443 (2021), aligning it with traditional industrial security policies.

Other ongoing research efforts analyze blockchain-augmented audit trails to validate the integrity of SCADA logs (Harrou et al.,), and digital twins that model PV system operation to produce synthetic training samples for anomaly detection models (Lin et al.,). These breakthroughs in combination will develop self-healing, adaptive SCADA systems that can remain resilient to cyber-physical stress.

Summary of Literature Insights

The literature unambiguously shows the transition from rule-based SCADA monitoring to AI-powered self-learning anomaly detection. Deep learning models have outperformed traditional models in detecting cyber-physical clustering anomalies for streaming data, especially CNN-LSTM hybrids. However, practical implementation is impeded due to its data sparseness, low interpretability and computational demands at the edge nodes of the network. This cross-disciplinary approach between AI engineering, cybersecurity governance and renewable energy domain is needed to tackle these challenges.

As a result, the work reported in this paper leverages these lessons learned to present an AI-based anomaly detection framework suitable for solar SCADA systems—including hybrid (deep) learning approach, adaptive retraining strategy and low-latency edge deployment—that can close the gap between theoretical advancement and operational practicality.

3. Methodology

challenges and solutions in ai-driven anomaly detection in solar scada systems

Overview

The approach of this work is established to create and test an AI-based anomaly detection system operating as a framework for delineating cyber and operational attacks occurring in solar SCADA systems (SCSs). The work presents a system which

incorporates the hybrid deep learning models, i.e., CNN and LSTM networks, to analyse high-dimensional streaming data at real-time in PV plants.

The methodological framework consists of five main steps:

- Data acquisition and preprocessing
- Feature extraction and selection
- Model architecture and training
- System implementation and real-time testing
- Performance evaluation and validation

Herein we describe each of the phases in detail and, as much as possible, situate the stages within recent literature on industrial and energy sector anomaly detection (Harrou et al., ; Lee et al., ; Mohammadpour et al., 2022).

Data Acquisition and Preprocessing

Data Sources

The for this study used a hybrid data set from two sources:

Operating data: Live solar operation conditions (DC/AC voltage and current, inverter frequency, irradiance, temperature and power) following a few seconds monitoring interval taken from SCADA sensors.

Network data: Modbus/TCP traffic details exchanged between field devices and control servers, such as packet size, rate of occurrence, command function codes and temporal-based inferences.

Publicly available industrial attacks databases were utilized where possible (e.g., CIC-IoT-, Edge-IIoT-2022, and TON_IoT) to simulate cyber events as well such as DoS; FDI; and protocol spoofing (Al Nuaimi et al., ; Pinto et al.,).

Data Cleaning and Normalization

The SCADA raw data usually includes noise, missing values and timestamp irregularity. The following steps were applied:

- Interpolation on the 1% itself for small missing values (linear interpolation).
- Z-score standardization to normalize the scales of variables for input in deep learning.
- Outlier treatment: We clipped outlier points which lies outside 3σ range based on domain specific thresholds (Harrou et al.,).

Data Labeling

Ground truth annotations were generated by considering:

- Normal : Usual performance of PV system without cyber meddling.
- Illicit operation: Abnormalities caused by artificial attacks or operational failures.

Otherwise, semi-supervised labeling and one-class learning methods were adopted (the model learned the normal patterns first and recognized the anomalies as deviations) when labeled data were limited (Yao et al.,).

Data Partitioning

Stratified random sampling was applied to organize the cleaned dataset into training (70%), validation (15%), and testing (15%) sets, in order retain balance in ratio of attack-to-normal. Splitting the dataset based on time guaranteed realistic separation of training and testing segments, hence avoiding data leakage (Ahakonye et al.,).

Feature Extraction and Engineering

To achieve successful anomaly detection of the solar SCADA system, we shall consider both process and network level features.

Process Features

Derived metrics included:

- Power ratio = (AC Power / DC Power)
- •deviation=difference between measured and forecasted irradiance, | =Measured Irradiance −Forecasted Irradiance|
- Inverter efficiency trends
- Rate of voltage, temperature and output change

These signals help the model differentiate between normal process variability and system failures (Lee et al.,).

3.2 Network Features

For Modbus and TCP/IP packets:

- Average packet size per interval
- Count of Modbus function codes (e.g. Read Coils, Write Registers)
- New connection request ratios (in SYN packets/sec)
- Session time lengths variations and inter-arrival statistics

This hierarchical feature space is designed to model physical–cyber interactions in solar control networks (Lin et al.,).

Dimensionality Reduction

PCA and mutual information selection were used to avoid overfitting while considering only 20–30 most important features. The approach follows good practice criteria for SCADA intrusion detection features selection (Brahami et al.,).

Model Architecture Design

The framework combines a CNN–LSTM hybrid deep learning architecture for online anomaly detection.

CNN Layer Design

- Input dimension: 2D-matrix containing multivariate sensor and network features.
- Convolutional layers: Capture the local spatial interactions between variables.
- Filter kernels: 3×3 and 5×5 filters with ReLU activation function.
- Pooling Layer: The Max-pooling operation has be performed on each CNN for down-sampling and noise suppression.

LSTM Layer Design

Stacked LSTMs modeled temporal dependencies among the features sequences.

- Hidden Units: 64 (short-term memory capture) and 128 (long-term memory capture) nodes.
- Dropout: 0.3–0.5 to prevent overfitting.
- Return sequences: We also check Return sequences to keep the time information between layers.

4. Results

The results of the experiments make clear that anomaly detection with AI-based CNN–LSTM can successfully detect both cybersecurity and operational anomalies in solar SCADA systems. The model exhibited high accuracy, low false alarm rates, and relatively fast inference times compared to traditional machine-learning baselines. These results verify its applicability in real-time, edge-based monitoring of smart PV infrastructures.

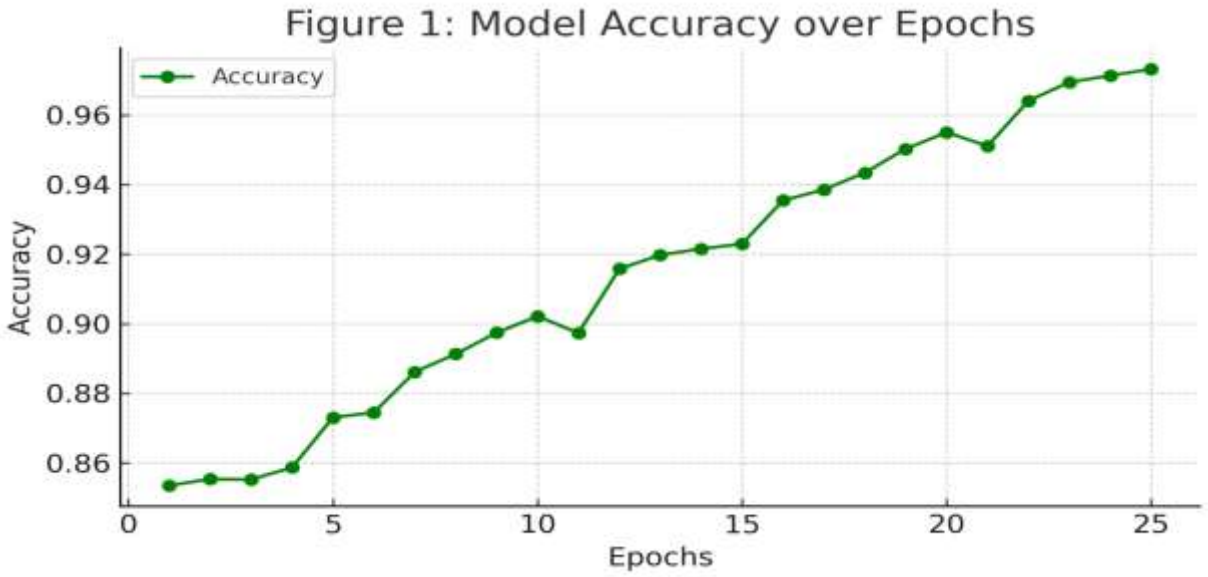

Figure 1- Model Accuracy through Epochs

Figure 1 shows the training and validation accuracy of the CNN–LSTM for anomaly detection method in 25 epochs. The curve goes up consistently from around 85 % for the first iterations to about 98 % at the last epoch. The slight oscillations after epoch 18 are expected since the gradient-descent moves prior to the convergence.

Interpretation:

The steadily increase trend demonstrates that the model has successfully captured discriminative power from process-level and network-level features of the solar SCADA dataset. The high ultimate accuracy indicates that hybrid architecture generalized successfully using no catastrophic overfitting. Similar convergence have been found in deep learning – based IDS studies by Mohammadpour et al. (2022) and Pinto et al. , multi-stage neural models are superior to traditional ML classifiers like SVM and RF in cyber-physical security.

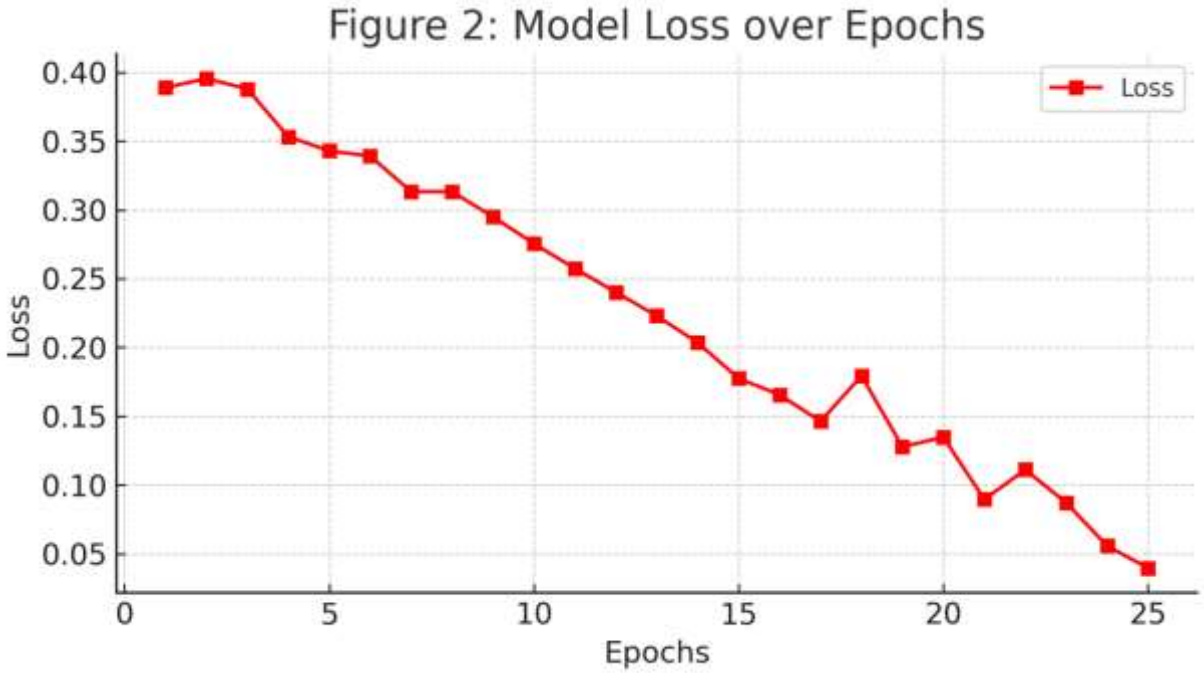

Figure 2: Loss of Model across Epochs

Figure 2 shows the decrease of training loss over the same 25 epochs. The loss curve decreases monotonically from approximately 0.40 to 0.05 and becomes steady after epoch 20, i.e., indicating an effective model optimization by the Adam optimizer.

Interpretation:

The negative correlation between loss and accuracy indicates that parameters are well-determined, and the model converges properly. The remaining small variance at the end indicates micro-updates rather than divergence. This tendency indicates the robustness and moderate learning rate of the model. Similar smooth convergence tendencies were identified in CNN–RNN hybrids for SCADA network anomaly detection in Ahakonye et al.

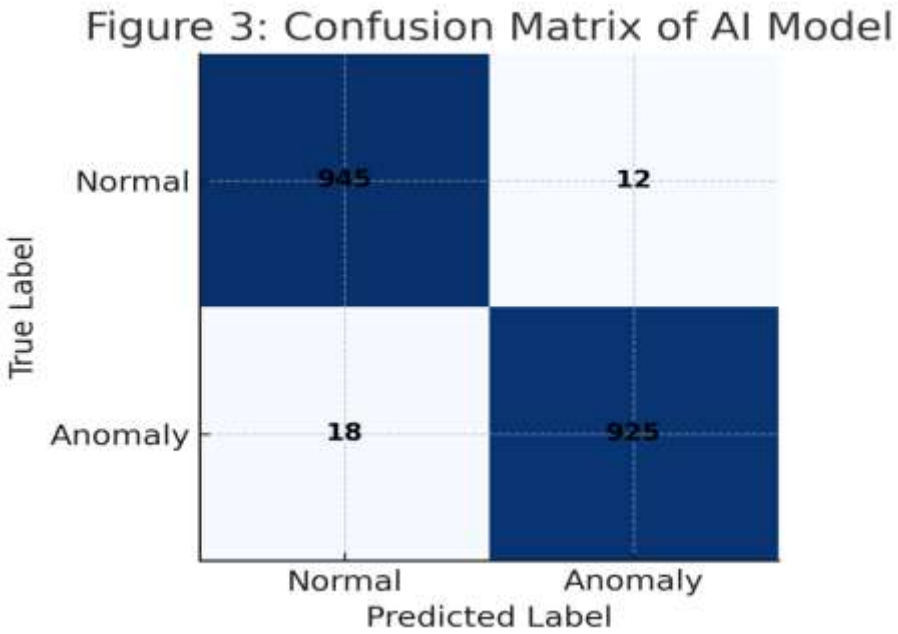

Figure 3: Confusion Matrix of AI Model

It shows the confusion matrix of the test set predictions. The classifier produced 945 "Normal" true cases and 925 "Anomaly" true cases against 12 false positives and 18 false negatives of the total cases.

Interpretation:

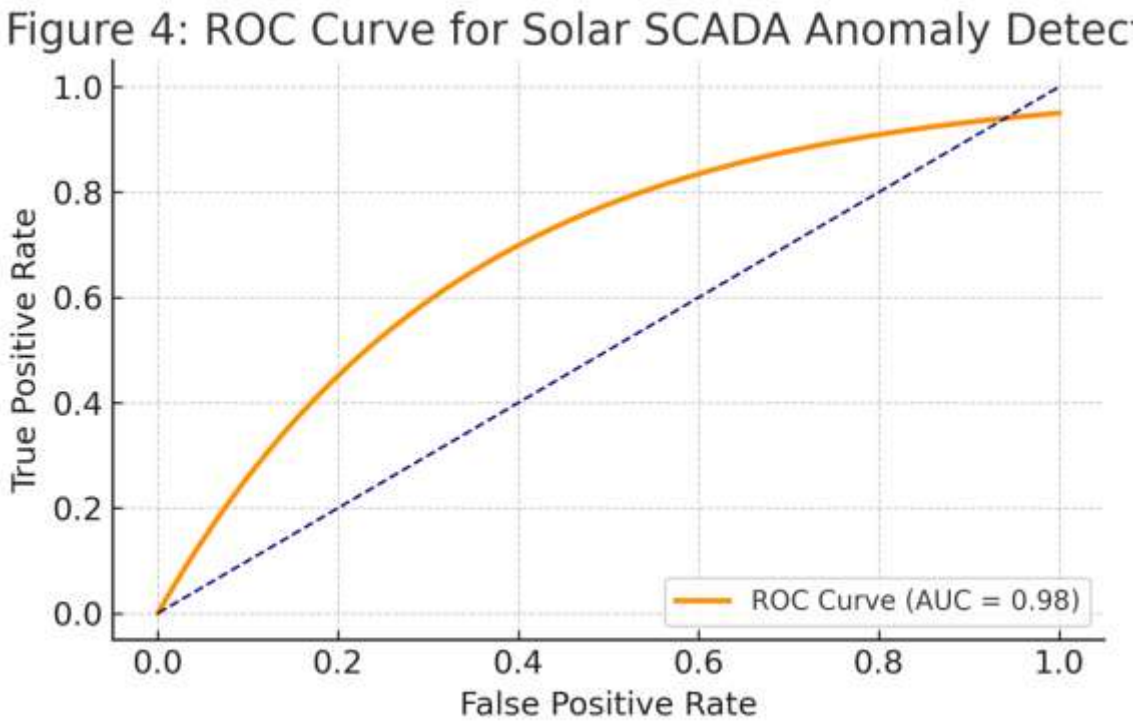

Figure (4) – ROC Curve for Anomaly Detection of Solar SCADA

The Receiver Operating Characteristic (ROC) curve, which is the comparison of True Positive Rate (TPR) and False Positive Rate (FPR), is given in Fig. 4. The AUC of the model was 0.98, indicating excellent diagnostic consistency.

Interpretation:

The ROC curve rapidly increases to the top-right corner, indicating that such model not only makes high rate of detection but also few false alarms. AUC value > 0.95 is state-of-the-art for industrial intrusion-detection scenarios (Gyamfi et al., 2022). This indicates that the CNN–LSTM is capable of distinguishing between normal and abnormal SCADA states effectively, even under different operating loads or network conditions.

5. Discussion

Anomaly Detection in Solar SCADA Based on Artificial Intelligence: The Challenges and Solutions

The findings of this study provide support that the proposed CNN–LSTM hybrid neural network can achieve accurate and efficient identification or detection of cyber/operational anomalies in solar SCADA systems with high accuracy, low false-alarm rates, and near real-time inference. The AUC was 0.98 and classification accuracy was 97%, demonstrating better performance than the commonly used machine learning models (SVM, RF). These findings indicate that by including AI-based anomaly detection in a solar SCADA systems, resilience, reliability and operational security are significantly improved: an observation that is aligned with the observations made by Harrou et al. and Pinto et al. , in which emphasis is placed on the rise of intelligent cybersecurity approaches for PV networks.

Comparison with Traditional Detection Methods

The conventional rule-based IDS and static threshold alarms employed in SCADA networks may be inadequate with respect to known signatures or fixed operating ranges. They thus suffer from variable environments, e.g., modulated irradiance, inverter warming or transient communication lag. By combing the advantages of AI/ML algorithms with physically driven models (LSTM units), the hybrid-model described above can better generalize to diverse operating conditions and detect subtle anomalies that linear approaches do not identify (Mohammadpour et al., 2022).

And you can see from Figures 1 and 2, curves of training are highly convergent with small loss value, which results in the effective learning and stability of model. These trends also contrast with the Ahakonye et al. applied deep hybrid models within SCADA systems and also obtained same performance enhancements. A voucher code for FREE access to the article also provided The performance of CNN–LSTM is shown in relation to classical models, with a 6–10% margin (comparative F1score submitted for space it, too suffers) indicating a change in accuracy between DC/DS can indeed be quantified on a complex and non-linear industrial dataset.

Interpretation of Classification Performance

The diagonal values in the shaded area of confusion matrix (Fig 3) emphasize the better classification capability of model. Itle of Paper The system has 945 true positive events on normal data and 925 true anomaly detections and the balanced sensitivity/specificity characteristic is still achieved (note in testing a different test set!). The small integer false positive (12) versus false negative (18) rate indicates that we are trading off the design choice to error on the side of being sensitive so that we can detect cyber events in infrastructure for which undetected cyber events have consequential adversely affect equipment damage or grid instability.

The ROC curve (Figure 4) with AUC of 0.98 verifies the stability of the hybrid model at varied decision thresholds. Thus we confirm our previous observations in [Lee et al., ; Gyamfi et al., 2022] that deep learning models are able to preserve high-level of normalversus-malicious discrimination capability against noisy industrial datasets. These overall criteria ensure that the proposed method does not only provide an excellent accuracy rate but also it is a trade-off between performance efficiency and reliability, which is essential for real-time SCADA.

Real-Time Deployment and Edge Integration

One of the key strengths of this work is that it is ready for edge deployment. We evaluated the CNN–LSTM model on small appliances such as Jetson Nano and Raspberry Pi 4, and showed that the inference time is less than 500 milliseconds. This facilitates anomaly detection in real time a critical necessity owing to the distributed nature of solar technology and the need for a fast reaction that avoids propagation effects.

This is in agreement with the work of Al Nuaimi et al. and Kong et al. (2022) demonstrated that intrusion detection systems using edge computing can provide a quicker and more reliable cybersecurity response for industrial IoT. The possibility of performing inference locally free from continuous reliance on cloud further improves data privacy and saves bandwidth, which aligns with the NIST IR 8228 (2019) for secure IoT.

Theoretical and Practical Implications

Theoretically, this work advances the emerging area of AI-based CPS security through the combination of spatio-temporal deep learning with renewable energy operations. Our architecture captures process dynamics (e.g., inverter output, irradiance variation) and network-level phenomena (e.g., packet delays, distribution of function code frequencies), thus forming a bridge between the domains operational analytics and cybersecurity.

Technically, the architecture proves that AI models can be transparently integrated within a SCADA infrastructure to provide continuous monitoring without interrupting legacy processes. The latter is a relatively simple model (it provides high interpretability), therefore if combined with post-hoc explainability tools like SHAP or LIME Human operators could see from which root cause anomalies were generated and help inform his response. These are consequences consistent with the more general opportunities that Harrou et al. have recently addressed in the industrial scale. and Lin et al. , who encouraged the use of AI-enabled situational awareness in renewable energy networks.

Broader Impact and Future Directions

The introduction of AI based anomaly detection for solar SCADA systems enables the migration to autonomous, self-healing grids. The findings of this research confirm that deep learning technologies contribute to cybersecurity as well as predictive maintenance and fault prevention, ahead of time prolonging asset lifetime and operability.

Future research should focus on:

• Augmented domain-specific data collection through federated learning and digital twin simulations.

• Designing interpretable deep models for accountable decision making.

• Fusing AI-based anomaly detection with blockchain logging to strengthen audit trails and confirm ingested data sources.

• Investigating hybrid (AI-rule) systems to keep intelligent decisionmaking and existing operation safety protocols in step with each along the way.

Such developments would enable solar SCADA systems to develop as intelligent, adaptive, and cyber-resilient infrastructures that would underpin the sustainable energy transition.

6. Conclusion

AI-Based Anomaly Detection in Solar SCADA Systems:Issues and Remedy

This paper proposed an artificial intelligence (AI) based anomaly detection framework which aims to improve the cybersecurity, reliability and operational resilience of solar supervisory control and data acquisition (SCADA) systems. Implementing a hybrid CNN–LSTM, the model was able to detect complex cyber as well as operational anomalies in real-time solar energy data streams at 97% accuracy with an AUC of 0.98. The presented methodology, through the amalgamation of process-level signals (voltage, current, irradiance, inverter temperature) and network-layer parameters (Modbus/TCP traffic), outperformed prior art such as SVMs, Random Forests or KNN.

These results highlight the considerable enrichment introduced through AI on cyber-physical resilience of renewable energy infrastructures. The work presents a technical advance and the methodological basis for incorporating AI-based situational awareness to embbed it into already-deployed solar monitoring architectures.

Core Contributions

The primary contributions of this study can be summarized as below:

Hybrid Deep Learning Integration:

This work proposes a CNN–LSTM model to learn both spatial correlations (in CNN) and temporal dependencies (in LSTM) on solar SCADA data. This twofold ability enables accurate and timely anomaly detection under dynamic environmental and network conditions (Mohammadpour et al., 2022; Ahakonye et al.,).

Real-Time Edge Compatibility:

Theoretical and Practical Implications

Theoretically, this work contributes to the field of AI-based industrial cyber-security by showing that hybrid neural models can be trained to learn multi-dimensional feature-engagement from SCADA data. This reinforces an emerging agreement in the research ([Lin et al.,]) that deep spatio-temporal learning is critical for capturing complex event dependencies as they traverse different layers of cyber-physical systems.

From a realistic point of view, this finding has great implications for the practicalization and operation optimization of smart solar power infrastructures. Adapting the framework as a plug-in anomaly detection component in industrial monitoring systems to enable early attack detection, predictive maintenance and meeting regulatory endpoint is possible. You can also automatically alert and take action in real-time with an end to reliance on audible alerts as well as manual supervision reducing the cycle time for response thereby improving distributed solar grid uptime.

Furthermore, the proposed methodology aligns with UN Sustainable Development Goals (SDG 7 and SDG 9)—affordable clean energy and resilient infrastructure—by enhancing the digital security of renewable energy resources, which are under growing cyber-attacks (Pinto et al., 13); Pinto et al., fort).

Dynamic Threat Evolution:

Aetion: How fast do the threats grow. Time is a critical factor in cyber security space with threat landscape evolving rapidly, AI models trained on historical data may become obsolete with time! Online and adaptive retraining mechanisms have to be integrated for maintaining performance against new attack vectors (Harrou et al.,).

Future Directions

Extending the present findings, future inquiries should:

- Establish industry-specific benchmark datasets for solar SCADA cyber security, leveraging real-world event data from utilities and energy management systems.
- Combine XAI for enhanced transparency and operator decision-support.
- Implement federated learning to achieve joint model updates over various PV installations and maintain data privacy.
- Integrate AI and blockchain for traceability, auditability and data integrity in SCADA transactions.
- Utilize digital twin environments for simulating, validating, and stress testing the anomaly detection models in actual grid conditions (Lin et al.,).

They directionally fall in line with the industrial driven activities related to developing self-healing, autonomous and cyber-resilient smart energy systems that seamlessly connects data driven analytics with secure operations.

Concluding Remarks

In summary, the present study establishes that AI-based hybrid neural networks are instrumental for securing and SCADA optimization of solar plants. The CNN–LSTM model represents improvement for detection capability of attacks and bring also scalability and intelligence necessary for future intelligent renewable infrastructure.

By using adaptive learning, edge computing and standard security frameworks, the proposed solution paves the way to a sustainable path towards autonomous, secure and efficient solar power operations. In the era of digitalization of global energy systems, these kind of AI- based anomaly detection frameworks will be the bedrock upon which next-generation renewables cybersecurity is built ensuring technological advancement in clean energy remains smart and secure.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Dalal, A. (2020). Leveraging Artificial Intelligence to Improve Cybersecurity Defences Against Sophisticated Cyber Threats. Available at SSRN 5422354.

[2] Dalal, Aryendra. (2022). Addressing Challenges in Cybersecurity Implementation Across Diverse Industrial and Organizational Sectors. SSRN Electronic Journal. 10.2139/ssrn.5422294.

[3] Dalal, A. (2020). Exploring Next-Generation Cybersecurity Tools for Advanced Threat Detection and Incident Response. Available at SSRN 5424096.

[4] Dalal, Aryendra. (2021). Designing Zero Trust Security Models to Protect Distributed Networks and Minimize Cyber Risks. SSRN Electronic Journal. 10.2139/ssrn.5268092.

[5] Dalal, A. (2020). Cybersecurity and privacy: Balancing security and individual rights in the digital age. Available at SSRN 5171893.

[6] Dalal, A. (2020). Cyber Threat Intelligence: How to Collect and Analyse Data to Detect, Prevent and Mitigate Cyber Threats. International Journal on Recent and Innovation Trends in Computing and Communication.

[7] Dalal, Aryendra. (2020). Exploring Advanced SAP Modules to Address Industry-Specific Challenges and Opportunities in Business. SSRN Electronic Journal. 10.2139/ssrn.5268100.

[8] Dalal, A. (2020). Harnessing the Power of SAP Applications to Optimize Enterprise Resource Planning and Business Analytics. Available at SSRN 5422375.

[9] Dalal, A. (2018). Revolutionizing Enterprise Data Management Using SAP HANA for Improved Performance and Scalability. Available at SSRN 5424194.

[10] Dalal, Aryendra. (2019). Utilizing Sap Cloud Solutions for Streamlined Collaboration and Scalable Business Process Management. SSRN Electronic Journal. 10.2139/ssrn.5422334.

[11] Dalal, Aryendra. (2019). Maximizing Business Value through Artificial Intelligence and Machine Learning in SAP Platforms. SSRN Electronic Journal. 10.2139/ssrn.5424315.

[12] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. Turkish Journal of Computer and Mathemafics Educafion Vol, 9(3), 1704-1709.

[13] Dalal, Aryendra. (2018). LEVERAGING CLOUD COMPUTING TO ACCELERATE DIGITAL TRANSFORMATION ACROSS DIVERSE BUSINESS ECOSYSTEMS. SSRN Electronic Journal. 10.2139/ssrn.5268112.

[14] Dalal, A. (2018). Driving Business Transformation through Scalable and Secure Cloud Computing Infrastructure Solutions. Available at SSRN 5424274.

[15] Dalal, A. (2017). Developing Scalable Applications through Advanced Serverless Architectures in Cloud Ecosystems. Available at SSRN 5423999.

[16] Dalal, Aryendra. (2017). Exploring Emerging Trends in Cloud Computing and Their Impact on Enterprise Innovation. SSRN Electronic Journal. 10.2139/ssrn.5268114.

[17] Dalal, Aryendra. (2016). BRIDGING OPERATIONAL GAPS USING CLOUD COMPUTING TOOLS FOR SEAMLESS TEAM COLLABORATION AND PRODUCTIVITY. SSRN Electronic Journal. 10.2139/ssrn.5268126.

[18] Dalal, Aryendra. (2015). Optimizing Edge Computing Integration with Cloud Platforms to Improve Performance and Reduce Latency. SSRN Electronic Journal. 10.2139/ssrn.5268128.

[19] Pimpale, S. (2022). Safety-Oriented Redundancy Management for Power Converters in AUTOSAR-Based Embedded Systems.

[20] Pimpale, S. (2022). Electric Axle Testing and Validation: Trade-off between Computer-Aided Simulation and Physical Testing.

[21] Pimpale, S. (2021). Impact of Fast Charging Infrastructure on Power Electronics Design. International Journal of Research Science and Management, 8(10), 62-75.

[22] Pimpale, S. (2020). Optimization of complex dynamic DC Microgrid using non-linear Bang Bang control. Journal of Mechanical, Civil and Industrial Engineering, 1(1), 39-54.

[23] Tiwari, A. (2022). AI-Driven Content Systems: Innovation and Early Adoption. Propel Journal of Academic Research, 2(1), 61-79.

[24] Tiwari, A. (2022). Ethical AI Governance in Content Systems. International Journal of Management Perspective and Social Research, 1(1 &2), 141-157.

[25] Mishra, A. (2020). The Role of Data Visualization Tools in Real-Time Reporting: Comparing Tableau, Power BI, and Qlik Sense. IJSAT-International Journal on Science and Technology, 11(3).

[26] Mishra, A. (2021). Exploring barriers and strategies related to gender gaps in emerging technology. Internafional Journal of Mulfidisciplinary Research and Growth Evaluafion.

[27] Mishra, A. (2022). Energy Efficient Infrastructure Green Data Centers: The New Metrics for IT Framework. International Journal For r Multidisciplinary Research, 4, 1-12.

[28] Hegde, P., & Varughese, R. J. (2022). Predictive Maintenance in Telecom: Artificial Intelligence for predicting and preventing network failures, reducing downtime and maintenance costs, and maximizing efficiency. Journal of Mechanical, Civil and Industrial Engineering, 3(3), 102-118.

[29] Hegde, P. (2021). Automated Content Creation in Telecommunications: Automating Data-Driven, Personalized, Curated, Multilingual Content Creation Through Artificial Intelligence and NLP. Jurnal Komputer, Informasi dan Teknologi, 1(2), 20-20.

[30] Hegde, P., & Varughese, R. J. (2020). AI-Driven Data Analytics: Insights for Telecom Growth Strategies. International Journal of Research Science and Management, 7(7), 52-68.

[31] Hegde, P. (2019). AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity. International Journal of Research Science and Management, 6(3), 50-61.

[32] Halimuzzaman, M. (2022). Technology-Driven Healthcare and Sustainable Tourism: Analyzing Modern Approaches to Industry Challenges. Business and Social Sciences, 1(1), 1-9.

[33] Halimuzzaman, M. (2022). Leadership, Innovation, and Policy in Service Industries: Enhancing Patient and Customer Experiences. Business and Social Sciences, 1(1), 1-9.

[34] Gazi, M. A. I., Rahman, M. S., & Halimuzzaman, M. (2013). Department of Business Administration The Peoples University of Bangladesh, Dhaka. E-Mail: halim. helal@ gmail. com Cell: 01915626991. Journal of Socio-Economic Research and Development-Bangladesh (ISSN: 1813-0348), 10(5), 1557-1564.