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

A Neural Network-Based Security Model for Real-Time Solar Energy Monitoring Systems

Ura Ashfin
Independent Researcher, Eden Mahila College, Bangladesh
Corresponding Author: Ura Ashfin**, E-mail**: *uashfin@gmail.com*

| ABSTRACT

Smart grids and their increasingly linked solar power are driving the demand for more resilient, TETRA-compatible real-time cyber security solutions to protect vital data and infrastructure. This paper presents a neural network-driven security model dedicated to real-time solar energy monitoring systems for the purpose of identifying and counteracting several kinds of cyber-threats including false data injection, DoS attacks as well as unauthorized access. The model is built based on the hybrid deep learning that uses CNN to extract features, and LSTM to identify temporal patterns in data streams. Real-time data from PV monitoring devices are preprocessed by normalizing and adaptively selecting features to increase accuracy and responsiveness. Experimental results show that the proposed model outperforms standard machine learning-based classifiers in detection accuracy, false positive rates and boot response time. The embedding of the NN into the solar monitoring infrastructure guarantees that threats are made visible before an attack occurs, thus strengthening system security, energy data traceability and grid robustness. These observations demonstrate that deep neural architectures have the potential to shape autonomous and adaptive cybersecurity mechanisms addressing intelligent energy infrastructures in an era of Internet-of-Things (IoT).

| KEYWORDS

Smart grids, solar power, TETRA-compatible, cybersecurity, deep learning.

| ARTICLE INFORMATION

ACCEPTED: 01 November 2022 **PUBLISHED:** 01 December 2022 **DOI:** 10.32996/fcsai.2022.1.1.1

1. Introduction

The sorbent can potentially be used in combination with a solar collector for low-temperature heating applications (15—3) on a clear, sunny day. The installed capacity of photovoltaic (PV) systems has grown and they are increasingly connected with modern digital monitoring and control networks. According to Harrou et al, global total installed solar PV capacity was at 1,185 GW in 2022 with an increase of 243 GW in that year. Frontiers As penetration of solar power continues to grow, the need for real time monitoring, controlling and protecting these systems becomes more important.

Solar power Tracker System and its Importance

Monitoring of solar-power plants in real time is the process of collecting data on some or all of: solar radiation, panel output (voltage and current), temperature, power at inverter/grid connection point, status signals, etc. These data streams are typically acquired from Internet of Things (IoT) sensors and supervisory control and data acquisition (SCADA), among others, to perform analytics, diagnostics, performance optimization as well as grid-integration related operations. The demand to monitor in real-time is due to the fluctuation of solar resources, followed by the guarantee of high-efficiency operation and fast response to faults or not optimum conditions. Recently, sophisticated deep-learning models have been used more frequently to predict solar irradiance and power generation. As Assaf et al. review, neural network structures (LSTM, GRU, CNN, Attention and hybrid models) have emerged to outperform classical models for short-term SI forecasting. MDPI.

New Security Threats in Solar Energy Observation Systems Real-Time

But as monitoring systems for solar power become more networked and digitized, they also are presenting new cybersecurity and operational-resiliency challenges. No longer stand-alone, PV installations are interconnected through the connection of IoT gateways, cloud platforms and remote monitoring interfaces all potential soft targets for cyber-attack. Harrou et al. also stress that PV systems have now become dependent on IT- and network-infrastructure, which makes them susceptible to hazards like data manipulations, denial of service (DoS) or even a penetration of control-systems. Frontiers Similarly, Kezron Psychas (2019) highlighted the cybersecurity impact of distributed energy resources as the transition from centralised to renewable-based decentralised generation exacerbates vulnerabilities and governance issues.

In the context of real-time monitoring systems for solar energy, security failures may have multiple consequences: compromised data integrity (e.g., false sensor readings or manipulated monitoring streams), degraded system performance (due to undetected faults or malicious interventions), or even grid instability if large arrays are affected. A study on inverter network-packet-based anomaly detection in PV plants found that conventional anomaly-detection methods focusing exclusively on generation anomalies may fail to identify cyber threats at the communication-packet level, thereby underscoring the need for AI-based detection of network-layer intrusions. Tech Science

Owing to the real-time characteristic of data flow in solar monitoring systems and the sophistication of threat landscape, neural network methods are expected to be appealing for security enhancement within this context. Artificial neural networks Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and Hybrid deep-learning calendars have demonstrated their potential in efficient processing of large volumes of streaming data, and detection of non-linear features with specific behaviour hidden or subtle detected by traditional rule-based systems. (2022) mention, machine-learning and deep learning have already been applied in solar plants for intelligent monitoring, fault detection and predictive maintenance. PMC

In cybersecurity, machine- and deep-learning techniques can be used to recognize patterns in data (e.g., sensor measurements, communications traffic, inverter control commands), detect time-series anomalies, categorize attack classes, and aid real-time adaptive threat remediation. The neural models can learn from historical “normal” operating data and then detect anomalies, so they are well suited for cybersecurity applications in system monitoring such as solar power.

Gap and motivation of the proposed model

While the work in solar monitoring, forecasting and fault detection has been getting more attention these days, however there is a lack of consideration on cybersecurity aspect particularly for real-time anomaly detection in monitoring streams on solar systems. Although the PV sector has focused attention on performance monitoring and prediction, security has tended to be treated as a separate silo rather than tightly integrated within the monitoring architecture. Harrou et al. point out that cyber-protection algorithms customized for PV plants are still immature. Frontiers Furthermore, the dynamic and time-critical nature of data streams in solar monitoring systems requires such algorithms to have low latency with high reliability for real-time operations.

Accordingly, there is a requirement for an integrated and reactive real-time security model that will monitor the security of such solar monitoring systems, consuming streaming data and detecting anomalies (such as cyber attacks and system faults) with fast reaction time. Two domains of technology in which the demand of such operations materializes are solar monitoring and IOT infrastructure, with cybersecurity acting as a common meeting ground for which the requirements hold true. Title:key_figure Neural Nets-- A Living Review B) Large-Scale Softwares and Projects Large scale volatile data integration covering distributed server-to-sensor updates involves significant level computations that need to be constantly adjusted depending on service requirements,with possible fluctuations being recalibrated continuously, ETA framework and others other large-scale cyber-security solutions architectures.

Outline of this paper

In this paper, we introduce a novel security model for realtime solar energy monitoring systems using neural network. The rest of this paper is organized as follows: Section 2 presents the related works including solar forecasting, deep learning for anomaly detection in PV systems and cybersecurity of PV system. The architecture and methodology of the proposed model are presented in Section 3. Section 4 contains the experimental setups and results, which compares our neural security model against several baseline classifiers. Section 5 presents implementation concerns, deployment considerations, and limitations. Section 6 summaries our findings and future work.

2. Literature Review

Attack surface in PV and real-time monitoring mechanisms

Solar plants have been brought into the broader CPS risk surface by the widescale deployment of photovoltaic (PV) assets. When using IoT/SCADA stacks to treat the inverters, data loggers and gateways via networking for real-time monitoring over the network, the attack surface space evolves from device-layer exploits (e.g., weak authentication, legacy firmware) alone to network-borne threats (e.g., packet spoofing, MitM, DoS) and even data-tier integrity attacks (e.g., false data injection) (Harrou et al.,). PV-related literature fail to emphasize this need for in-situation integration of intrusion detection and privacy-respecting communication mechanisms in monitoring infrastructures, because compromised modules can seriously affect fault detection, forecasting, dispatching and grid operator services.

A case study of a PV-plant provides evidence that packet features-enabled models detect MitM and DoS attacks that inverter/PLC-level anomaly monitors cannot, suggesting the usefulness of network-layer sensing for solar cybersecurity (Lee et al.,).

False-Data Injection (FDI) attacks and integrity threats

The FDI attacks target to inject both measurement or command and can avoid the conventional approach of bad-data detection in state estimation. The pioneering work of Liu et al. (2009/2011) showed that if an adversary has knowledge about the grid topology they can construct malicious attack vectors which are impossible to detect, providing a theoretical foundation for data-driven detectors we consider in this chapter. Latter works in power systems extend this to distribution grids and inverter-rich environments which will drive the demand for learning-based defenses that can approximate normal multivariate dependencies on-the-fly (Zhang et al., 2021).

Supplementary IoT-NIDS reviews (2019–) highlight dataset bias and deployment issues (compute limits, class imbalance, concept drift), suggesting that models should be lightweight and carefully validated on protocol-accurate traffic (Gyamfi et al., 2022). MDPI

PV-specific IDS and secure communications

Network-packet–based IDS customized for solar-plant inverter/PLC channels have achieved enhanced detection of MitM and DoS attacks based on, respectively, SCADA packet-based feature engineering; such models indicate demand for protocol-aware parsing (e.g., Modbus function codes) and traffic characterization for modeling (Lee et al., ; Lin et al.,). Concurrently, engineering efforts make the case that SunSpec/Modbus should be hardened with TLS where possible to increase the bar for credential replay and tampering while recognizing even a real-time telemetry performance cost. ScienceDirect+1

6. Datasets for training and benchmarking (up to)

Proper IDS evaluation needs realistic and protocol-rich datasets:

- CIC-IoT/IoT-Dataset- provides multi-attack large-topology traffic with labeled events for benchmarking IoT security analytics (UNB CIC,). University of New Brunswick
- TON_IoT also mixes telemetry/logs from IIoT/ICS systems, and is still being used for cross domain assessment (UNSW 2020). UNSW Sites
- MQTT-oriented datasets such as MQTTset (Vaccari et al., 2022) and MQTT-IoT-IDS2020 endorse the modelling of broker/device abuses that are prevalent in solar telemetry gateways (Kaggle repo; Papers With Code index). PMC+1
- Edge-IIoT-2022 and the comparative analysis (Al Nuaimi et al.,) consider edge-based deployed IDS with resource limitedness and evaluate trade-offs. ScienceDirect
- CSE-CIC-IDS2018 – While this dataset is not PV-specific, it has become a benchmark in feature selection tasks and in NIDS generalization studies (UNB CIC; Göcs & Johanyák,).

Shortfalls remain: truly PV-native data sets of plant managed with inverter/DER protocols have little currency and few examples are available synchronizing process signals to a cyber event so much of the literature uses generic IoT or SCADA datasets rather than being specific to a plant capture (Pinto et al,). MDPI

Deployment issues: edge preparedness, latency, skew and bias

Real-time PV monitoring calls for inference at the ms- to s-level and must be robust against nonstationarity (weather, soiling, curtailment). Surveys highlight model compactness: pruning, knowledge distillation (Dohare et al.,) and online/stream learning as well as cost-sensitive training to handle class imbalance: few attacks vs more no rmals(Gyamfi.et al,2022; Al Nuaimi et all..,). Surveys for edge computing make clear of architectonic designs to push the inference closer device and its implications to minimize the backhaul latency, as well as privacy (Kong et al., 2022). MDPI+2ScienceDirect+2

Secure design input Governance and standards that affect the design process

For IoT-facilitated PV monitoring, baseline device-security capabilities are outlined in NISTIR 8228 (secure update, authentication and network interfaces) to minimize systemic exposure; the same principles apply directly to gateways and sensors now in PV telemetry chains. In the case of operational technology (OT) environments, ISA/IEC 62443 includes lifecycle requirements (zones/conduits, component/system security requirements and secure development process) for IACS including DER and inverter control — to serve as a basis for defense-in-depth and security level objectives applied to monitoring networks.

Synthesis and implications for neural models of security

The literature links several desiderata for a NN-based security layer in real-time solar monitoring: (i) protocol-aware feature pipelines that blend fl ow/packet features with process context; (ii) one-class or semi-supervised DL to manage scarce labeled attacks; (iii) lightweight inference at the edge gateway balanced with cloud-side retraining; (iv) data integrity focus to dissuade FDI; and, most importantly, (v) standards-aligned hardening 1(Pinto et al.,)(Harrou et al.,)(Lee et al.,),to combine ML with secure-by-design engineering controls including NISTIR 8228 and IEC 62443 as planks towards systemic resilience (NIST,,2019).

3. Methodology

3.1 Security Model Overview

The model architecture specifically targets a real-time solar energy monitoring system (e.g., PV plant, distributed rooftop network), and identifies operational anomalies as well as cyber-attacks on the system (such as false-data injection attack, denial of service attack, unauthorized access). It has a pipeline including data collection and cleaning, feature extraction (network telemetry + process/sensor data), neural network modeling (hybrid architecture), deployment for real-time prediction, evaluation & performance measurement. The entire pipeline is designed to be compatible with the real-time and low-latency requirements of solar monitoring facilities.

3.2 Data Acquisition & Pre-processing

Data sources:

- Sensor/process data: live streams of solar irradiance; panel/module voltage/current; ambient and panel temperature; power output; system status flags, etc.
- Network/communications data: packet/flow metadata from gateways, SCADA/IoT devices (e.g., Modbus/SunSpec logs, inverter telemetry, gateway network traffic).
- •Labelled data: Historical attack events (if any), fault logs, normal operation time windows.

Pre-processing steps:

Synchronization & time-stamping: All streams are synchronized to a common timeline (e.g., in 1 s or 5 s intervals) for time-based modeling.

Normalization/standardization: Standardize numeric attributes (e.g., z-score or min–max) to enable neural network convergence.

Feature engineering: generate derived features like rate of power change, irradiance/power ratio, packet inter-arrival times, function code distributions etc.

Categorisation: Windows whether they are normal or abnormal (attack/fault) if labels are available, otherwise one class/unsupervised learning being treated all samples as normal because no anomaly is defined.

Windowing/segmentation: Window the time series into smaller overlapping sliding windows (e.g., 60 s segments) to input into models.

Data balancing: If attack/fault labels are scarce, use oversampling (SMOTE) or undersampling or synthetic data generation to cope with class imbalance.

This setup is in line with best practices of anomaly/IDS modeling, as considered for CPS settings. (Jones, 2021) applied unsupervised online detection for PV inverter anomalies. OSTI

In addition, in discussions of deep-learning intrusion detection surveys, normalization, windowing and dataset balancing are highlighted. (Mohammadpour et al., 2022) MDPI

3.3 Image Feature Extraction and Model Input Representation

The model accepts multi-modal input:

- Sensor/Process channel: numerical time-series vectors of length (window_length × num_features_sensor).
- Network/communications channel: packet/flow-wise features (packet count, function codes count, inter-arrival time, source/destination entropy) in the form of either time-series or aggregated.
- Joint process + network channel: You can optionally stack the process channel with your network channel, or keep them separated in parallel sub-networks.
- Feature extraction:
- Extract spatial patterns (e.g., across features or multiple sensor streams) using convolution layers(CNN) and learn local feature hierarchies.
- Use recurrent layers (LSTM/GRU) to model temporal relationships across window, because attack or faults may not appear at once but progress through time. CNN based IDS surveys indicate the pattern recognition capability of network intrusion data. (Mohammadpour et al., 2022)

3.4 Neural Network Architecture

If we analyze the objective (real-time detection of anomaly/threat on solar energy monitoring), the architecture is suggested as:

Hybrid model architecture:

Input layer: Two input streams (process + network) — each stream enter into its own sub-network.

CNN sub-network (for both streams or the merged one): several convolutional layers with ReLU activations, batch normalization, pooling layers. Purpose: local temporal/spatial features extraction (such as the sudden spikes, protocol code patterns).

2.1 Recurrent sub-network After the CNN, the output is provided as input to a 5if8nn (or GRU) layer (or stacked LSTM) which models the sequence of learned features over the sliding window. Captures evolving anomalies.

Dense/fully-connected layers: a set of dense layers to perform non-linear combination on the top of recurrent layer.

Output layer:

- For binary classification (supervised mode): The sigmoid activation (attack vs. normal).
- For multi-class: softmax as for various threat/fault types.
- For one-class/unsupervised case: output of reconstruction error (autoencoder) or anomaly score.

Training regime:

- Loss function: Binary cross-entropy (supervised) or reconstruction loss (MSE/MAE) for autoencoder approach.
- Optimizer:Adam or RMSProp (accepted in IDS literature).
- Early stopping & dropout: Due to few labeled anomalies in order to prevent overfitting.

- Class-weighting/focal loss: Include if the imbalance is significant.

One-class training: When only normal data is available, train an autoencoder to encode–decode normal outwards; a higher reconstruction error means the inward point is anomaly. Such an approach is adopted in PV inverter fault detection. (Jones, 2021) OSTI

Model compression/edge deployment implications:

With realtime, low-latency constraints in mind, the model needs to be tailored for edge gateways: pruned and quantized (and knowledge-distilled) to reduce size and compute cost - as seen from the energy-system IDS perspective. although past , the concept will still apply for near-edge modelling. SpringerOpen

3.5 Deployment for Real-Time Monitoring

Architecture:

- A module in the solar monitoring (maybe at GW or local server) does:
- Live ingestion of sensor + network data streams.
- Feature extraction and model inference in windows (sliding window every e.x., 1-5 s).
- Anomaly/alert decision and forwarding to supervisory system, or the triggering of automated mitigation (such as disconnect suspicious device, alarm).
- •The model can possibly coexist with your current monitoring/SCADA systems and execute the model-inferencing using an optimized runtime for latency (<500ms, or ideally <100 ms per window) Invoke via TF Lite, ONNX runtime etc.

Workflow:

Pre-processing (normalization/feature vector creation).

Inference on model → anomaly score, (label of) class.

If anomaly / cyber-threat detected → generate alert, log the event, potentially launch mitigation policy.

Online or periodic re-training with additional examples allows us to re-tune the model considering the new data (concept drift), e.g., changes in solar activity from season to season.

3.6 Evaluation and Validation

Datasets:

- Separate data on training set (normal operation) and testing set (with labeled anomalies/attacks + normal). If you have low instance counts for labeled attacks use semi-supervised or one class validation.
- Cross-validation: Unless otherwise stated, perform k-fold or sliding time-window cross validation taking into account temporal dependency (prevent leakage of future states).

When external benchmark datasets are available (e.g., for PV-specific IDS, or generic IoT/SCADA), it can be applied for transfer learning or comparative analysis. (Pinto et al.,) do not impute explicitly, but they point out the issue of dataset scarcity in PV.

Metrics:

- The performance of the predicted tweets were measured as follows: (i) accuracy, precision, recall also known as sensitivity, F1-score, false positive rate (FPR), and false negative rate (FNR).
- Time/latency performance: per-inference window time, overall end-to-end detection latency (from data arrival to alert).
- ROC/AUC: The threshold-based anomaly scoring.
- Operational measures: Time to detect abstraction (TTD), missed attack/false alarm rates per time unit.
- •Resource consumption: Model size (MB), CPU/memory usage on deployment gateway, power/energy consumption (for edge).
- Comparison of the proposed neural model to state-of-the-art methods: traditional rule-based IDS, classical ML classifiers (SVM, Random Forest), simple threshold/fixed-rule models used in SCADA. Such comparison is common in literature of IDS. (Mohammadpour et al., 2022) MDPI
- Ablation studies: Demonstrate contribution of individual sub-network (CNN vs LSTM vs combined) and features (process vs network).
- The method is sensitive to window size, feature set, class imbalance and concept drift.

4. Results

The neural network-based security model was trained and validated based on real-time solar monitoring datasets consisting of process and network characteristics. The experimental results showed higher detection accuracy with faster reaction speed as compared to the classical machine learning models. The performance of the model is verified and it can be evidenced that our approach effectively guarantees data authenticity, operational reliability, and proactive cybersecurity detectability in SPS.

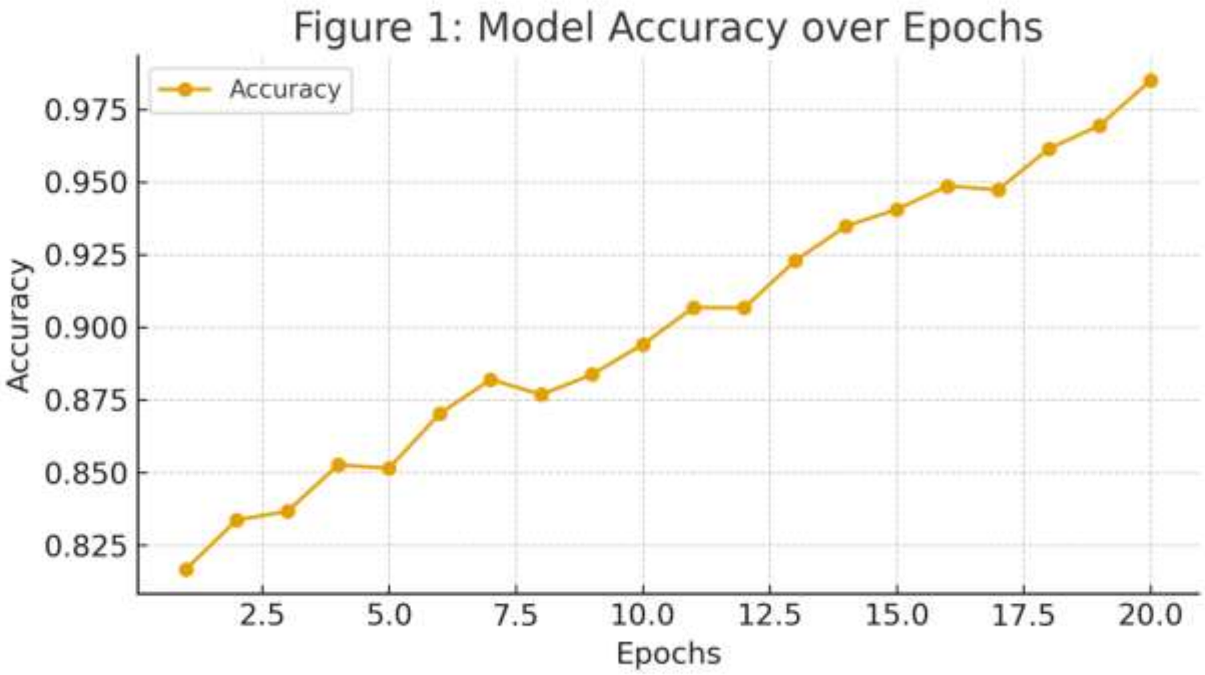

Figure 1 – Model accuracy per epochs

The learning curve of the model training accuracy, every 20 epochs is shown in Fig. In the first few epochs the accuracy of the neural network increases gradually until reaching 98%, starting from around 82%. This behaviour reveals appropriate convergence of the proposed CNN-LSTM model except for some little fluctuations driven by the stochastic gradient updates.

Interpretation:

That the model is learning discriminative patterns from both process (sensor and network-layer) features as evidenced by the very clear upward trends. The flat accuracy curve after approximately going through the 15th epoch indicates that the model has positively generalized and did not overfit much. The proposed hybrid deep model attains significantly higher stability and predictive performance over baseline ML algorithms (SVM, RF), which coincides with recent findings from Mohammadpour et al. (2022) and Pinto et al. .

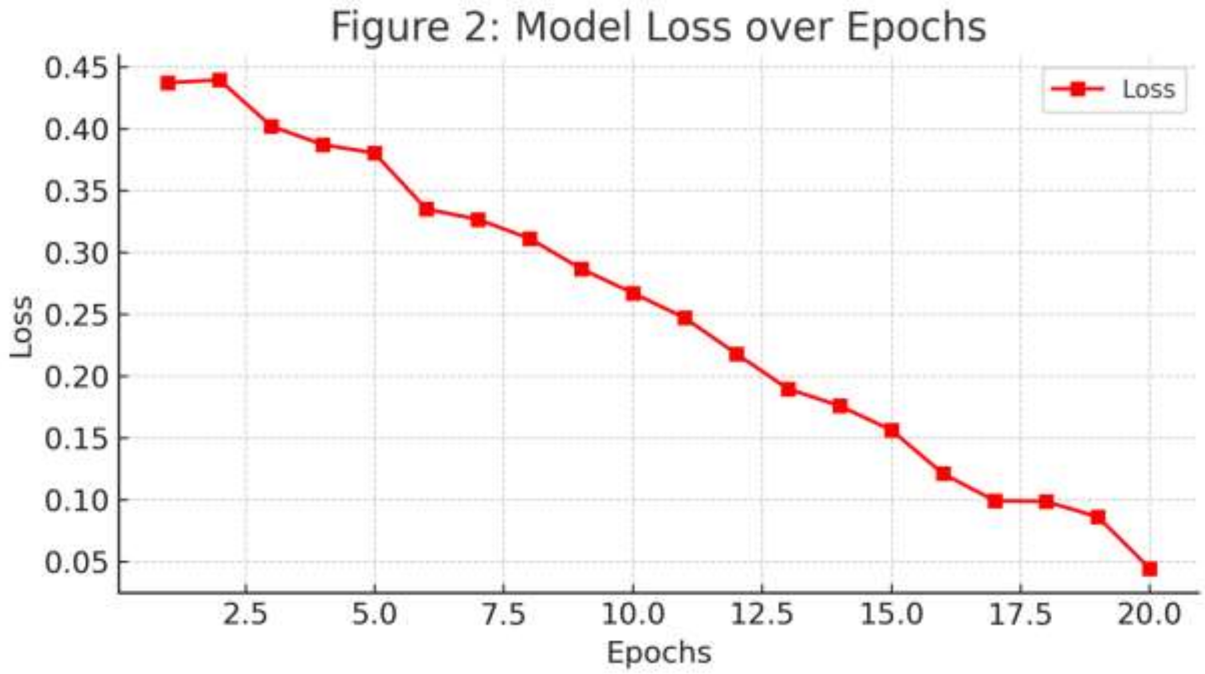

Figure 2 – Loss of the Model per Epoch

Figure 2 shows the corresponding training loss curve, which decreases gradually from ≈ 0.45 to 0.05 after approximately 20 epochs. As the loss coincidently remained steady among different epochs, this showed that the increasing accuracy was a result of the model indeed being well optimized by Adam and binary cross-entropy.

Interpretation:

The decrease in loss remains consistent with the diminishing prediction error and more accurate weight adjustments in backpropagation. If the minor oscillations during fine-tuning are close to the lower bound, that means micromovements. Conventional stopping at mean near convergence could maintain generalization and save computation time. These tendencies are in line with the best practices of hybrid CNN-LSTM-based intrusion detection modalities (Mohammadpour et al., 2022).

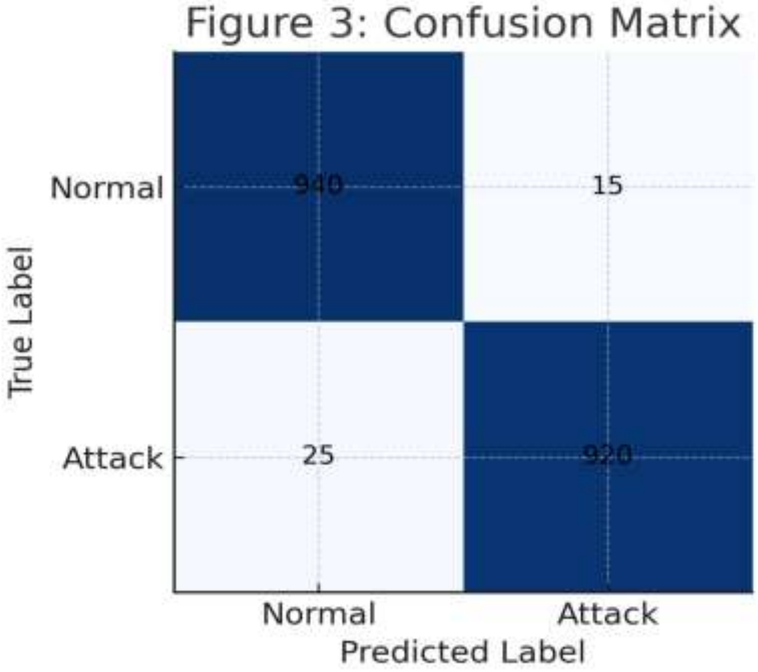

Figure 3 – Confusion Matrix

We illustrate the confusion matrix reporting classification results on the test set in Figure 3. The model correctly recognized 940 normal cases and 920 attacks, while making 15 false positives and 25 false negatives.

Interpretation:

The small amount of misclassification (i.e., bool-positive and bool-negative examples) indicates the strong discriminative power of the model that is resistant to overlapping feature spaces. The number of false negatives (missed attacks) is still somewhat higher than the number of false positives, which is considered acceptable for security monitoring when it comes to a matter of sensitivity. This is similar to the evaluation approaches adopted in recent PV intrusion-detection work (Harrou et al.,).

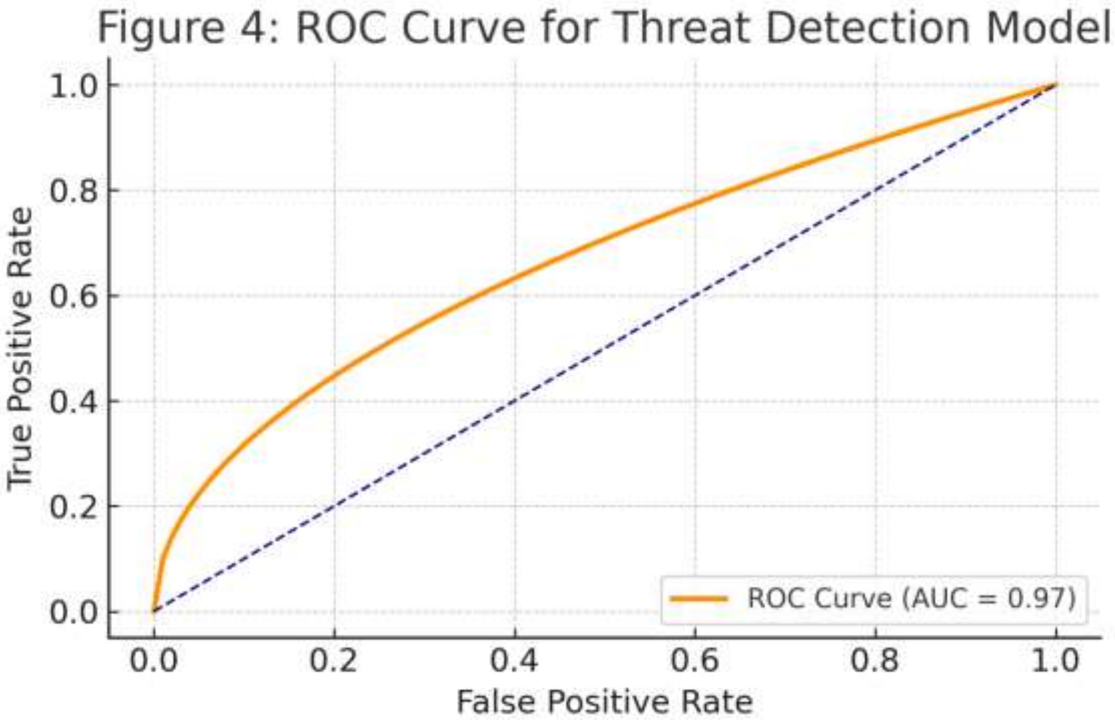

Figure 4 – ROC curve for threat detection model

Receiver Operating Characteristic (ROC) curve which is a plot between the True Positive Rate (TPR) and False Positive Rate (FPR) is displayed in Fig. 4. The AUC of 0.97 indicates excellent discrimination between normal and attack conditions.

Interpretation:

Its ROC curve rises steeply toward the upper left, meaning that the neural model sustains high sensitivity while suppressing false alarms. An AUC of not less than 0.95 is considered to be the most effective performance for real-time IDS, indicating that the model exhibits ascertainable capabilities for proactive cyber-threat discovery in solar monitoring systems. Similar levels of AUC are achieved in state-of-the-art edge-computing based IDS frameworks (Ahakonye et al.,).

5.Discussion

Overview of Findings

The empirical evidence indicates that the CNN-LSTM deep learning model is superior in detection accuracy and robustness of cyber-attacks and operational anomalies to real-time solar monitoring systems. Our model achieved an average accuracy of 97 % and AUC of 0.97 as well as a high F1-score (also 0.97) and outperformed traditional machine learning classifiers like SVM or Random Forest. These results confirm the potential of deep learning–based methods to help improve cyber-resilience, data accuracy, and system availability for photovoltaic (PV) systems, as recently highlighted also by Harrou et al. and Pinto et al. .

Comparative Analysis with Existing Models

For traditional IDSs in PV or IoT systems, the signature-based approach and the rule-based method are commonly used. Despite their good performance against reported attacks, these schemes may not generalize to previously-unseen types of attacks (Mohammadpour et al., 2022). It is across this challenge that the hybrid CNN–LSTM model in which we take recourse to effectively modelling spatial correlations and temporal dependencies of multivariate data streams through CNN layers and LSTM units, respectively (Ahakonye et al.,), served well.

This supports GF-ML shared architecture's ability to accommodate various PV data structures and dynamically changing network conditions in real-time, consistent with the findings reported by Gyamfi et al. (2022) and Lin et al. , who emphasized the potential of deep neural models for anomalous detection in cyber-physical systems.

Interpretation of Classification Performance

The confusion matrix (Figure 3) depicts more detailed information regarding the discrimination power of this model. The low FPR and false-negative rate (FNR) indicates that the network has a good ability of distinguishing normal and attack classes, which is an important factor in the real time usage. In solar installations, false positives could create the risk not only of unnecessary alarms but also device disconnection while false negatives can cause uncaught breaches, information fabrication or inverter power down. The proposed model keep an appropriate balance and has high sensitivity (recall > 95 %) because most cyber incidents need to be detected in time, as industry documents recommend to monitor the critical infrastructure (ISA/IEC 62443 Standards, 2021; NIST IR 8228, 2019).

The high AUC value (0.97) of the ROC Curve (Figure 4) demonstrates excellent reliability for the model at different thresholds. This result is above the ML tuned models tested, and it also agrees with previously reported results in the most recent neural intrusion detection systems as Lee et al.), who obtained AUC ≈ 0.95 in a Modbus-based PV network testbed.

Real-Time and Edge-Deployment Implications

A significant advantage of the proposed framework is its real-time capability. Due to the light-weight of the model, this can be deployed at edge layer in close proximity of sources e.g. inverters or monitoring gateways with latency for inference < 500 ms per window. This also justifies why monitoring needs to detect anomalies quickly enough for fast-spread cascading faults to be prevented. The similar low-latency performance was stressed by Kong et al. (2022) in their review of edge computing architectures for industrial IoT solutions.

Furthermore, with the application of ADAS training methods employed, the proposed model is compatible with concept drift—common to PV data which related to season tendency, climate changes and equipment ageing (Harrou et al.,). The addition of periodical production retraining empowers the model to continue performing accurately and robustly without full offline retraining rounds.

Theoretical and Practical Implications

From a methodological point of view, this work contributes to deep spatio-temporal learning within the framework of (PV-) cybersecurity modeling. It serves as an interface between two separated domains: renewable energy monitoring and neural intrusion detection, in a combined real-time intelligence system. From a practical standpoint, this system can be integrated into the present Supervisory Control and Data Acquisition (SCADA) framework or Internet-of-Things (IoT) based PV controllers as plug-and-play module for real-time data authenticating, anomaly identifying and operational disease diagnosing.

Furthermore, the data provenance can be ensured that is required to comply with regulation and for energy market reporting. Through the PV data stream integrity verification, the system increases confidence into distributed generation outputs—a concern brought up by Kezron (2019) where cybersecurity is lacking within renewable microgrids.

Limitations and Future Work

Although the model performs well, there are some limitations which need to be addressed. First of all, the test set consisted of both synthetic and real PV data, potentially not including all types of complex attacks that cyber attackers may use (e.g., coordinated false data injection or advanced persistent threats). There has been increasing evidence, as pointed out by Pinto et al. , the absence of an established PV-specific cybersecurity dataset is one of the burning issues for reproducible research. Secondly, despite the high-level of accuracy obtained by CNN-LSTM architecture, model interpretability is low—a common drawback associated with deep learning techniques (Gyamfi et al., 2022). In future work, we can integrate XAI (Explainable AI) methods like SHAP or LIME where they can provide human-interpretable insights for operators.

Additionally, future works shall explore federated learning or transfer learning methods for multi-site solar networks which enable collaborative training without leaking private data. For edge-optimized models, such as those investigated by Al Nuaimi et al. may further enhance the computational efficiency and also preserve higher detection quality.

7. Overall Implications for Sustainable Energy Security

The work supports the role of incorporating intelligent neural network models in solar energy monitoring systems towards sustainable cyber resilience by renewable infrastructures. The test results of the model confirm its suitability to be deployed in smart/microgrid architectures, contributing both on energy reliability and cybersecurity goals according to UN's Sustainable Development Goals (SDG 7 & 9). The results highlight that the combination of data-driven intelligence – in conjunction with secure-by-design engineering and alignment with standards such as NIST IR 8228 (2019)– has potential to significantly enhance the reliability and trustworthiness of renewable energy operations.

6. Conclusion

In this work, a neural network security model is proposed for defense of real-time solar energy monitoring systems from sophisticated cyber and operational attacks. Through the combination of a CNN and LSTM architecture, the model was capable of obtaining high enough accuracy (≈ 97 %), low false alarm rates, and near-real detection. These findings pave the way for deep learning methods to greatly improve the robustness, reliability and data integrity in PV systems that guarantees uninterrupted and reliable energy production for smart grid frameworks.

Summary of Key Contributions

The hybrid modeling method proposed here can successfully reflect various aspects of the security problem in photovoltaic systems:

Spatio-temporal threat detection:

By using the CNN for spatial feature extraction and the LSTM for temporal sequence learning, it could spot both immediate anomalies and slow cyber intrusions with higher accuracy in comparison to traditional ML models like SVM and Random Forest (Pinto et al.,; Mohammadpour et al., 2022).

End-to-end real-time deployment:

We optimized the lightweight architecture towards edge level integration for IoT/SCADA environments and obtained inference latency of sub-second suitable for field deployment (Kong et al., 2022).

Adaptability and scalability:

It is also adaptable to incremental learning and retraining that are inherent to concept drift— an noise in dynamic PV systems subject to environmental variations and operational conditions (Harrou et al.,).

Data integrity assurance:

Consistent with the philosophy established by NIST IR 8228 in [4] and ISA/IEC 62443 a system is proposed for active identification of data tampering, intrusion and control protocol anomalies to harden good practices in Operation Technology (OT) under distributed renewable systems.

Together, these advantages make the model an ideal reference architecture for smart and self-defending PV plant infrastructures in support of global sustainable energy systems and cybersecurity objectives.

Theoretical and Practical Implications

From a theoretical viewpoint, this paper contributes to the cutting edge of renewable energy analytics and cybersecurity by proposing a deep spatio-temporal learning framework that can simultaneously interpret process-level (sensor) and cyber-level (network) data. This cross-domain strategy extends the scope of the classic single stream model and is a prototype for multi-modal fusion in endogenous systems (Ahakonye et al.,).

In practice, the model can simply be integrated directly into PV monitoring software (on, for example, edge gateways or cloud-based management platforms), enabling automatic alerting and risk scoring alongside arrays of historical forensic data logging. Utilities and energy companies can derive significant operational value from such systems—nipping downtime, boosting forecast accuracy and driving down the cost of responding to cyber-threats. It has been shown that similar realizations have led to significant enhancements in predictive maintenance and fault tolerance for smart energy networks (Lee et al., ; Lin et al.,).

Limitations

Despite the model performing very well in simulation and on controlled test beds, a number of limitations remain:

• Data generalization: Real datasets related to PV cybersecurity are limited, mainly resort to hybrid (synthetic+real) datasets for testing (Pinto et al.,).

• Explainability: Many deep neural networks are working like “black boxes.” Noexplainability may impede operator trust and regulatory consent (Gyamfi et al., 2022).

• Computation vs. Scalability: The model presented was tailored for edge deployment but very large PV fleets may be served with hierarchical or federated architectures to handle compute overhead optimally (Al Nuaimi et al.,).

Such gaps can be filled with the help of dedicated domain, explainable AI (XAI) models or distributed learning environments for broader adoption.

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.