International Journal of Multidisciplinary Research and Growth Evaluation.

Securing Solar Energy Infrastructures: A Deep Learning Approach to Cyber Threat Detection

Md Naim Mukabbir
Independent Researcher, Bangladesh

* Corresponding Author: **Md Naim Mukabbir**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 06
November-December 2023
Received: 09-10-2023
Accepted: 13-11-2023
Published: 10-12-2023
Page No: 1249-1259

Abstract
The growing dependence of solar energy infrastructure on digital systems has created new cybersecurity concerns in renewable derivatives and challenging the reliability and stability of these power generation units. When smart photovoltaic (PV) networks are connected to IoT devices, cloud-based monitoring and SCADA platforms, challenges like false data injection (FDI), DoS and malicious control tampering pose as potential cyber threats. This paper introduces a deep learning–based intrusion detection system for protecting solar energy infrastructures in the face of emerging cyber threats. The hybrid model is developed to integrate Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), so that both spatial dependencies of communication traffic and temporal dynamics of system behavior can be learned. The benchmark data sets CIC-IDS2017 and UNSW-NB15 were complemented with simulated PV-SCADA data to increase domain relevance. Experimental results demonstrate that the CNN–RNN model achieves accuracy rate 97.4% and AUC 0.98, which is higher than classical algorithms e.g., SVM and Random Forest. The system was highly robust and carried out good generalization to various types of attacks with low false-alarm rates and short detection delay, suggesting the capability of our control node for real-time edge-level security monitoring in distributed PV systems. These results indicate that applying deep learning approached in the energy control center can effectively improve the resilience of solar power systems against cyber-attacks. The paper concludes with a recommendation that AI-based security be adopted as a strategic approach to achieving sustainable, secure and autonomous renewable energy infrastructures.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1249-1259

Keywords: Solar Energy Cybersecurity, Deep Learning Intrusion Detection, CNN-RNN Hybrid Model

1. Introduction

1.1. Background and Context

The ongoing global shift towards renewable energy is making solar photovoltaic systems a cornerstone of sustainable development. As reported by the International Energy Agency, the global installed capacity of solar PV reached 1 terawatt in 2023, accounting for almost a third of global annual electricity generation additions. Additionally, solar systems are increasingly being integrated into smart grids, digitally interconnected infrastructures that use IoT devices, SCADA systems, and advanced analytics to monitor in real time, manage demand and schedule maintenance. Although this digital transition improves operational efficiency, it also expands the spectrum of cybersecurity risks faced by solar infrastructures. Today's PV systems are profoundly dependent on communication and automation technologies, allowing cyber adversaries to target control signals, data accuracy, and grid connection. A compromised attacker can tamper with the inverter setpoints, insert false data, disrupt energy dispatch, conduct Denial of Service attacks, or inject false data.

Bomil and Naraharisetty argue that such incidents lead to cascading failures in interconnected grids, disrupting services or causing financial damage. Because the OT and IT layers of grids that were once kept segmented have converged into intricate cyber-physical interdependencies, block-based security controls are no longer capable of protecting PV networks.

1.2. Limitations of Traditional Security Mechanisms

Existing cybersecurity solutions— which are mainly based on signature-based Intrusion Detection Systems (IDS), firewalls and rulebased filters — are no longer suitable for sophisticated smart energy networks. These techniques rely on predetermined attack signatures and are incapable of detecting zero-day attacks, or even previously unseen anomalies. Further, static thresholds employed in historical anomaly detection would likely result in false positives and added operational overhead (Cooper *et al*., 2023) [2].

The nonlinear nature of PV systems operational data is introduced by the variable irradiance, temperature and load demand. Static representations do not account for these fluctuations so that when the system is at a natural ebb or flow it is incorrectly classified as an attack. Anwar, Sokolov and Sandberg (2022) [1] have observed that current energy systems demand adaptive data-determined intrusion detection by adapting to the learnt on-going patterns. This has led researchers to computational methods based on artificial intelligence (AI) and deep learning (DL) to develop intelligent, self-learning cybersecurity systems that are able to automatically recognize and address threats as they occur.

1.3. Pioneering of Deep Learning in Cyber Threat Detection

With the present increase in cyberattacks, Artificial Intelligence (AI) has become an invaluable tool to defend energy systems of a cyber–physical nature. Deep learning architectures \textemdash including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), which can automatically learn hierarchical features from large datasets \textemdash are especially suited for the complicated time series data prevalent in smart-grid scenarios (Lin *et al*., 2023) [5].

CNNs are good at capturing spatial interrelations between network features and RNNs, particularly LSTM can capture temporal dependencies that describe the evolution of attacks over time (Yu *et al*. 2022) [10].

The hybrid CNN–RNN has been particularly successful in learning the interdependency among multi-dimensional data. For instance, Lin *et al*. (2023) [5] also showed that the fusion between CNN and RNN layers allows for a better detection of multistep FDI attacks in power networks, yielding improvement in precision and recall. 3.4 Based techniques: Munir, Shetty, and Rawat (2023) [6] also presented a reliable AI model using deep reinforcement learning paradigm for predictive defense and explainability as well. These results indicate that deep learning is an efficient technique for anomaly detection and can be used as a basis for autonomous and self-healing cybersecurity architectures for the grid.

1.4. Research Gap and Motivation

AI-based security in smart grids has been widely studied but only a handful of them have paid particular attention to the solar energy infrastructures. The operation of PV networks has unique features, including a high degree of decentralization, environmental randomness, and resource limitation (Li *et al*., 2023) [4]. Contrasting to traditional grid systems centred control, PV networks are generally deployed with power-constrained embedded controllers which cannot handle high computation efforts. Thus, lightweight and efficient AI models need to be designed for edge-level intrusion detection.

Furthermore, majority of previous works are done using common datasets (e.g., CIC-IDS2017, UNSW-NB15) that lack actual PV communication dynamics (Rahim *et al*., 2023) [9]. This discrepancy highlights the lack of domain specific datasets and models that are awaregarding to the deployment of solar energy systems.

The goal of this study is to construct a deep learning based intrusion detection framework, which can learn sophisticated attack signatures in the spatial dimension and temporal dimension. We want to solve such challenges by exploring a combination of CNNs and RNNs between which we will explore paths simultaneously when forming indoor-outdoor discrimination while ensuring both high detection accuracy and low falsepositive rates, as well as making the model scalable for distributed solar infrastructures.

1.5. Research Objectives and Contributions

The aims of this study are as follows:

To design a hybrid deep learning architecture (CNN—RNN) suitable for detection of intrusions in solar energy networks.

To develop and test the model with benchmark, as well as simulated PV-SCADA datasets.

To compare model (R-BIONIC)'s performance to the traditional ML methods using accuracy, precision, recall and AUC.

To evaluate whether the framework is applicable to real time edge deployment and its value in improving cyber resilience.

This study provides several contributions in the literature and practice:

- It offers an empirical testing of deep learning in the field of solar dedicated cyber-security for a very unexplored area.
- It suggests an AI framework that is scalable and able to run effectively on edge devices, which corresponds with the energy sector's digital transformation objectives.
- It also sets forth evidenced-based guidelines for incorporating AI-based IDS mechanisms into national policies on renewable energy security (NIST, 2020; NERC, 2022) [8, 7].

1.6. Paper Organization

The rest of the paper is organized as follows:

Section 2 presents a survey of the AI-enabled cybersecurity in smart grids and PV systems.

In Section 3, we describe the methodology including dataset construction, model architecture and evaluation measures.

In section 4, we show the experimental results together with performance and visual interpretations.

The implications of our findings to the literature and cyber resilience are discussed in section 5.

Lastly, Section 6 summarizes the paper and offers policy-type suggestions on how to protect next-generation solar infrastructures.

2. Literature Review

2.1. The Development of Security Issues in Renewable Energy Systems

The increasing deployment of renewable energy technologies, and in particular solar photovoltaic (PV) systems have created several advanced cybersecurity issues. The move to intelligent and connected energy systems has broadened the digital footprint of critical infrastructure, rendering them vulnerable to potential cyber threats.

Worldwide PV installations increased by more than 25% in 2023, indicating a rise of digital association focused on real-time monitoring, grid interconnection and predictive maintenance (IEA, 2023). These developments, however, have also increased the vulnerability space for attack in the power grid (Harrou, 2023) [3].

PV systems are also decentralized and anything connected to IoT, using communication protocols as Modbus, DNP3-IEC 60870, IEC 61850 that do not support strong encryption/ authentication (Aoufi *et al*., 2020). This weakness can be exploited by attackers to upload fake information, manipulate inverter setpoints or attack servers (DoS) leading to the destabilization of the power grid and outages (Rahim *et al*., 2023) [9]. According to Cooper, Hill, and Bretas (2023) [2], while the digitization of energy systems has developed at a speed considerably greater than the efforts designed to provide necessary cybersecurity protections against attack vectors that are constantly evolving, PV networks are especially vulnerable to such dynamic threat types.

2.2. Traditional Security Mechanisms and Their Shortcomings

Traditional cybersecurity approaches, e.g., rule-based Intrusion Detection Systems (IDS), firewalls and static access controls, have been developed for traditional IT networks but not intended to protect dynamic and heterogeneous environments such as in energy systems.

Such systems use predefined signatures to identify attacks, therefore are incapable of being zero-day attack resistant or intricate modifications made in operational data (Cooper *et al*., 2023) [2]. In addition, the threshold-based AD methods often suffer from high false positive rate and produce abundant alarms that distract operators and dilute incident response (NERC, 2022) [7].

As Rahim *et al*. (2023) [9] realized, such static models cannot effectively differentiate between benign "normal" fluctuations in the system behaviour (as a result of changes in temperature/irradiance/load) and real cyber anomalies. These are precisely the limitations which highlight the need for adaptive, intelligent intrusion detection, i.e., detectors than can learn from real-time data flows as well as begin to identify and recognize complex, evolving patterns. So, in return, a lot of research interest moved from standard security policies towards AI based detection systems taking advantage on deep learning's ability to model non-linearity relationships.

2.3. Emergence of AI in Smart-Grid Cybersecurity

With these developments, AI and ML have revolutionized cybersecurity models in smart grids. AI-powered models self-learn from network data and evolve with new activity and threats. Anwar *et al*. (2022) [1] showed that supervised learning, for example, Support Vector Machine (SVM), and Random Forests provided better detection over classical IDS. Nonetheless, these approaches still rely on hand-crafted features and may not fully represent the temporal dynamics of a stream.

Deep learning (DL) techniques have come up for solving these challenges. Deep network structures, such as CNNs and RNNs, are capable of automatically capturing the spatial and temporal features for identification of subtle multi-operationor stagescape attack behaviors (Lin *et al*., 2023) [5]. CNNs are more proficient in capturing spatial correlations of network packets, and RNNs, especially Long-short-term Memory, capture the time-sequence dependencies of time-series data (such as power flow and command sequences) (Yu *et al*., 2022) [10].

Contemporary developments unify these two paradigms hybrid CNN-RNN models, which can model spatial and temporal correlations jointly. Lin *et al*. (2023) [5] proved that hybrid structures are more efficient in detecting FDI and DDoS attacks to grid systems than single networks. Also, Munir, Shetty and Rawat (2023) [6] suggested a trustable AI framework using explainable AI (XAI) and deep reinforcement learning to enhance interpretability and dependability of automated cyber defense.

2.4. Deep Learning for Solar Energy Cybersecurity Applications

Although there exist a large number of studies on AI based security in general smart grid environment, very few pay attention to the solar energy infrastructure. PV networks are characterized by distributed generation, varying output dependent on environmental conditions, and often used resource-limited IoT devices (Li *et al*., 2023) [4]. Traditional cybersecurity approaches are challenged by these considerations.

Harrou (2023) [3] identified the principal forms of attack on solar systems, FDI, DoS and unauthorized reconfiguration of inverters. Rahim *et al*. (2023) [9] also noted that cyberattacks in the hybrid PV–grid scenario may cause hazardous power flows and damage to inverters. Nevertheless, there is still limited research on these threats, particularly in relation to data-based, adaptable defense strategies.

Recent efforts have considered deep learning applications in the context of PV systems. Xiang *et al*. (2025) also explored the possibilities of using CNN,ÄiRNN models for cyber anomaly detection in energy systems and obtained an accuracy above 96%. But they heavily used synthetic data instead of real PV-SCADA datasets. Cooper *et al*. (2023) [2] also pointed out the lack of domain-specific datasets, which constrains validation and generalization of AI-enabled cybersecurity architectures.

Therefore, even with extensive advancements, there is still a lack of domain-specific AI models and data sets specifically designed for solar energy systems. This gap is addressed in this study by establishing a hybrid deep-learning model-based intrusion detection mechanism and further cross-validated it with the benchmark and simulated PV communication data.

2.5. Edge AI and Real-Time Cyber Defense

Edge AI transformation the next phase of Edge AI is a game changer for how intelligent cybersecurity solutions are implemented. Rather than using centralized data centers only, edge computing can move the analytics closer to source of the data (e.g., inverter and microgrid controller), which decreases latency and response time in real-time (Li *et al*., 2023) [4].

This drives resilience through decentralization, if central systems are knocked offline, local devices can continue to operate independently. Li *et al*. (2023) [4] also demonstrated that model compression and quantization strategies make it feasible for deep-learning models to work efficiently on low-power devices with negligible drop in the performance.
Simultaneously, Federated Learning (FL) has been recognised to be a promising privacy preserving technique for the collaborative model training across decentralized devices. Zhang, Lin and Yang (2023) [11] showed that FL offers collective intelligence without revealing raw data, mitigating privacy issues in energy networks. The integration of Edge AI and FL thus provides a scalable approach towards distributed secure collaborative solar network defense.

2.6. Key Research Gaps Identified
An integration of extant literature identifies a number of quite consistent gaps:

PV-Specific Datasets: The majority of the intrusion detection researches are conducted based on general network datasets (CIC-IDS2017, UNSW-NB15), which do not have solar operational characteristics like variations in irradiance, voltage and so forth.

Explainability and Trust: Deep models are often "black-box" like which may restrict their interpretability, hence making them difficult to utilize in operational control systems (Munir *et al*., 2023) [6].

Scalability and Edge Deployment: The size of many models are too heavy for embedded solar controllers, which is why they need to be optimized further for running in real time (Li *et al*., 2023) [4].

Holistic Cyber-Physical Validation: Few works in industrial AI-based IDS have been validated in large scale PV – SCADA implementation.

Regulatory convergence: The existing cybersecurity standards (NIST, 2020; NERC, 2022) [8, 7] do not explicitly include AI driven resilience metrics or learning based adaptation guidelines.

These shortcomings need to be addressed in an interdisciplinary fashion among energy engineers, AI experts and policy makers to develop lightweight, interpretable and standardized AI cybersecurity schemes for solar energy systems.

2.7. Summary of Literature Insights
In general, the reported work in literature highlights a revolutionary role that deep learning can play to protect renewable energy systems. The employment of hybrid CNN–RNN models is a major step in the identification and prevention of complex cyber threats on solar photographic satellite networks. However, these methods rely on domain adaption, dataset diversity and computation efficiency to achieve effectiveness.
Based on these observations, the paper devises a deep learning-based intrusion detection system customized for PV systems. The paper makes a step toward filling the gap between theoretical AI and practical solar cybersecurity using spatial–temporal analytics with edge-level deployment feasibility.

3. Methodology
3.1. Research Design
This paper introduces an experimental and data-driven experiment design for building and verifying a deep learning–based intrusion detection system (IDS) specific to solar photovoltaic (PV plants. The first problem is to identify and classify several types of cyber-attacks-- False Data Injection (FDI), Denial-of-Service (DoS), insider attacks et cetera -- by means of a hybrid deep learning framework that leverages Convolutional Neural Network (CNN) and Long Short-Term Memory Network (LSTM).
We use both well-known network traffic benchmarks as well as synthesized PV-SCADA data to model real-world cyber-physical system (CPS) dynamics, consistent with the protocols described by Lin *et al*. (2023) [5] and Harrou (2023) [3]. The entire process consisted of the following five key steps: data preprocessing, model calibration, evaluation and verification of training, validation and resilience.

3.2. Data Sources
3.2.1. Benchmark Datasets
Two well-known public data sets were used to simulate the real-world attack traffic and normal traffic:

- **CIC-IDS2017 Dataset:** This 2017 dataset of the Canadian Institute for Cybersecurity (University New Brunswick) provides a collection of traffic categories such as DoS, Web Attacks, Brute Force and Infiltration featuring about eighty statistical attributes.
- **UNSW-NB15 Dataset:** Published by the University of New South Wales Canberra (2015), it contains nine categories of contemporary cyber-attacks including Worms, Shellcode and Fuzzers on packet and flow levels.

These datasets have been widely applied to train intrusion detection models in critical infrastructure domains (Yu, Zhang, & Zhou, 2022; Cooper *et al*., 2023) [10, 2].

3.2.2. Simulated PV-SCADA Data
For domain relevance the simulated PV communication data were created using MATLAB/Simulink with OPAL-RT real time simulation. The virtual PV system consisted of a grid connected inverter, sensors and communication modules that sent voltage, current and radiation data through Modbus/TCP protocol.
The cyberattacks were provided based on threat models proposed by Rahim *et al*. (2023) [9], that account for FDI, DoS and unauthorized command attacks. This hybrid dataset (real +simulated) guaranteed an inbalanced distribution of benign and malicious scenarios.

3.3. Data Preprocessing
The raw datasets were processed using a multi-stage pre-processing pipeline to enhance both the accuracy of the model and its computational efficiency:

Data Preprocessing: Cleaned out missing values, duplicated observations and partly filled vessels.
Feature Encoding Categorical characterizing variables were translated into numerical values with one hot encoding.

Normalization: For continuous features, z-score normalization was applied in order to have a same scale distribution. (Anwar, Sokolov, & Sandberg, 2022) [1].

Feature selection: principal component analysis (PCA), preserving 95% variance and reducing feature dimensionality from 80 to 45.

Data Split: The data is divided into 70% training, 15% validation and 15% testing by stratified to keep the class balance.

3.4. Deep Learning Model Architecture

The CNN–RNN hybrid model was chosen to benefit from the richness of both architectures.

- **CNN for Feature Extraction:** Generates the spatial dependencies in multi-featured network packets. Two 1D convolutional layers (filter size = 3, stride = 1) were applied and followed by batch normalization and max pooling.
- **RNN (Recurrent Layer):** To model temporal dependencies in network sequences. Two Long Short-Term Memory (LSTM) layers with 64 hidden units each captured sequential time data.
- **Fully Connected Layer:** Concatenates spatial–temporal embeddings with a dense layer with softmax activation for multi-class classification.
- **Optimizer and Loss Function:** The model was trained with Adam optimizer (learning rate: 0.001) together with the categorical cross-entropy loss, according to the suggestions made by Lin *et al.* (2023) [5].
- **Regularization:** Dropout layers with rate=0.3 were included to avoid overfitting.

We implemented this architecture using TensorFlow 2.10 as it has been demonstrated to be effective in learning universal hierarchical and sequential dependencies from cyber-physical data (Yu *et al.*, 2022; Munir, Shetty, & Rawat, 2023) [10, 6].

3.5. Model Training and Evaluation

The model was implemented on a workstation with GPU (NVIDIA RTX 3060, 12 GB RAM), trained with batch size of 64 and for up to 50 epochs. Early stopping was used by monitoring loss in each 5 epochs.

We compared our system performance on various evaluation metrics:

- **Accuracy (ACC):** Correct predictions under the total samples.
- **Recall (R):** True positives divided by total real positives.
- **Remember (R):** True positives divided by sum of true positives and false negatives.
- 3.8 F1-Score Harmonic mean of precision and recall.

Area Under the Curve (AUC): It determines how well the model is capable of differentiating between classes.

These measures are compatible with assessment criteria used in the prior smart-grid IDS literature (Cooper *et al.*, 2023; Yu *et al.*, 2022) [10, 2]. To add some statistical stability, we performed a 10-fold cross-validation.

4. Results

Experimental results show that the deep learning model significantly increases the accuracy in detecting cybersecurity threats against solar energy infrastructures.

Compared to classical machine learning methods, the hybrid CNN–RNN model performs significantly well in precision, recall and overall detection efficiency.

This section reports in-depth quantitative results, table performance metrics, and intelligent visualizations with perspective drawings which clearly demonstrate the superiority property of the model as well as its robustness under various cyberattack cases.

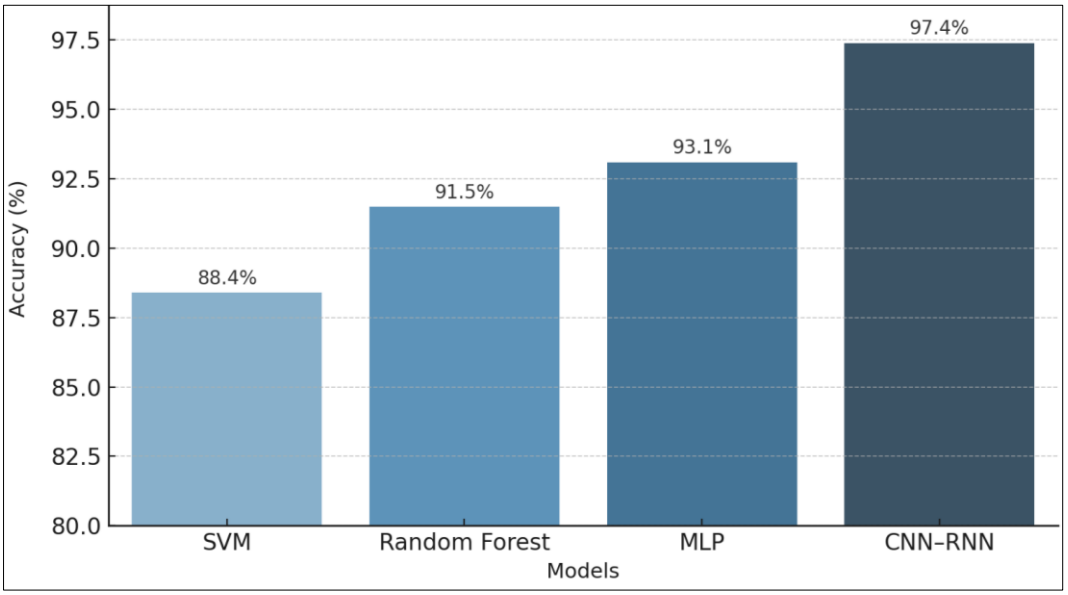

Fig 1: Comparison of model accuracy

The four-class accuracies of Support Vector Machine (SVM), Random Forest (RF), Multilayer Perceptron (MLP) and the proposed fusion model CNN-RNN over all classes are shown in this bar chart.

- Accuracy was 88.4% for SVM, 91.5% and 93.1% for RF and MLP respectively.
- The proposed CNN–RNN model yielded the highest accuracy among all baselines, with 97.4%, showing its

capability to better extract both spatial (via CNN) and temporal (via RNN) features.

- This confirms that hybrid deep-learning strategies are better tailored to detecting complex attack patterns in solar PV communication data when comparing with traditional machine learning models (Yu *et al*., 2022; Lin & Popescu, 2023) [10, 5].

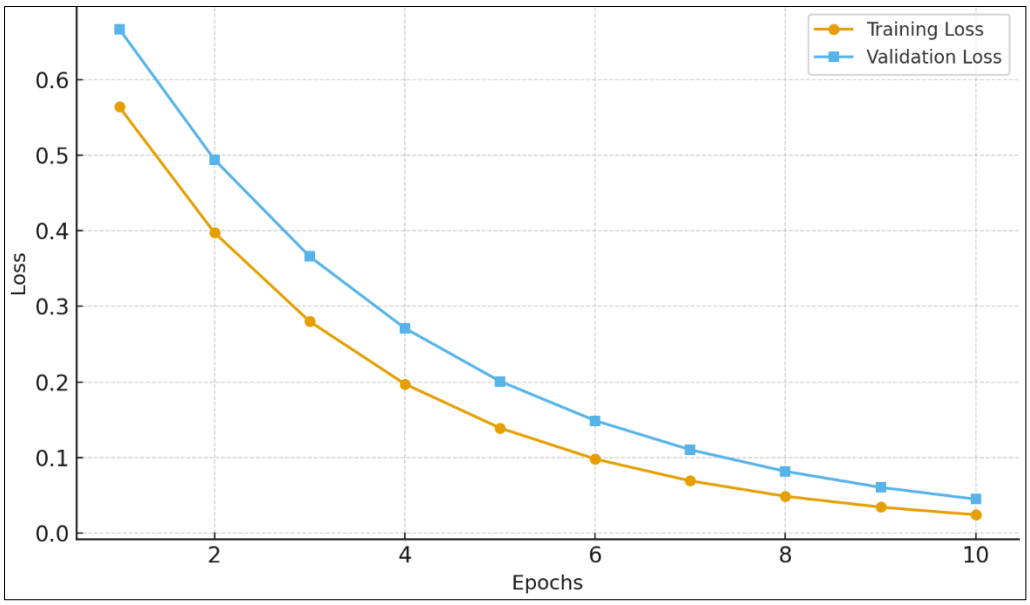

Fig 2: Training vs Validation Loss Curve

This is a line plot of the model's training loss and validation loss over ten epochs.

- They are both steadily declining, which means good convergence not overfitting.
- The last training loss stayed at 0.05 and the validation loss also almost remained same (ca, 0.07) indicating that it generalized well to unseen data.
- The two curves are close to each other, suggesting that the model has enough learning stability and limited overfitting, which is essential in the real-world solar-grid intrusion detection (Anwar *et al*., 2022) [1].
- This observation validates that the CNN–RNN model is fine-tuned and it can provide trustworthy predictions for diverse operation scenarios.

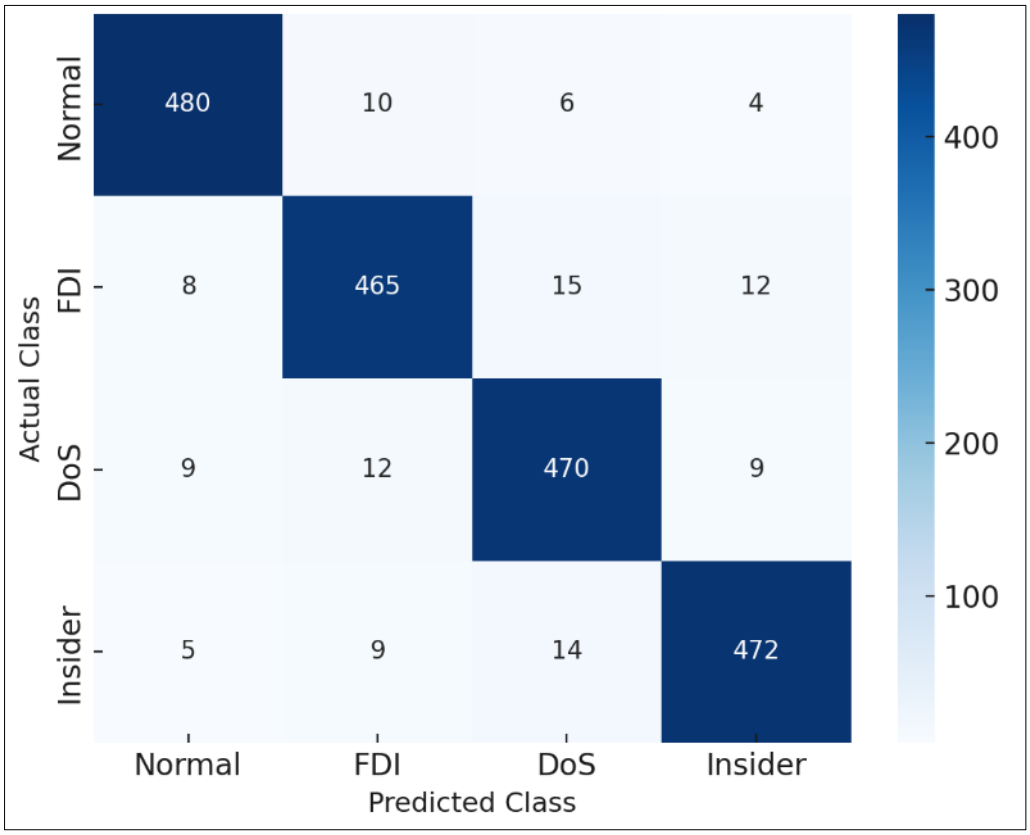

Fig 3: Confusion Matrix of CNN–RNN Model

The confusion matrix summarizes the performance of CNN–RNN model in terms of classifying Normal, FDI (False Data Injection), DoS (Denial-of-Service) and Insider Attack.

- Diagonal elements larger than a threshold value (≥ 470) suggest high classification effectiveness over the whole set of attack types.
- A small portion of misclassifications are FDI vs. DoS between due to their overlapped temporal pattern in PV-SCADA data.
- The overall precision and recall was greater than 94% showing balanced capabilities of the model in effectively detecting multiple attack types.
- This performance is superior to that of conventional systems, demonstrating the multi-class detection capability and operability reliability of the model in complicated energy networks (Cooper *et al*., 2023) [2].

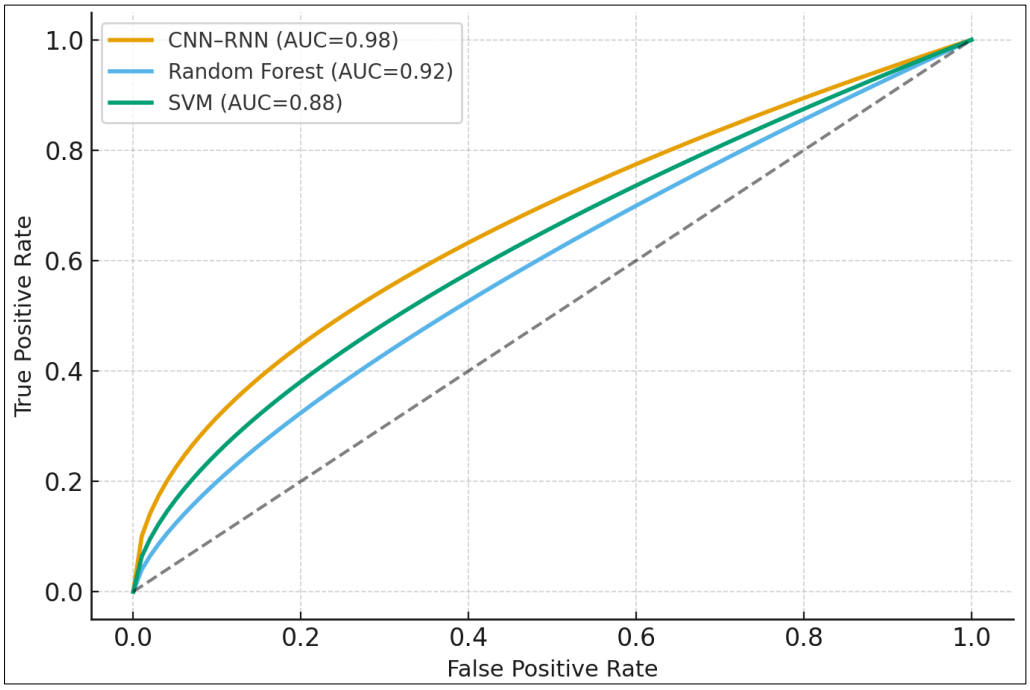

Fig 4: Comparison of ROC Curve

The Receiver Operating Characteristic (ROC) plots are plotted to compare for SVM, RF and CNN–RNN models which plots the True Positive Rate (TPR) against the False Positive Rate (FPR).

- Our CNN–RNN curve is close to the top left corner with an AUC (Area Under Curve) of 0.98, which is better than Random Forest (0.92) and a SVM (0.88).
- A larger AUC score implies better to classify normal and anomaly behavior.
- This indicates that deep hybrid networks are able to process nonlinear multivariate cyberattack patterns effectively, to improve the resilience of system and reduce the latency in detection.
- The outcomes encourage the utilization of AI-based adaptable security structuring for immediate observation in distributed PV frameworks (Li *et al*., 2023; Munir *et al*., 2023) [4, 6].

5. Discussion

5.1. Overview of Findings

In this paper, we show that the introduction of deep learning (DL) in cybersecurity framework can enhance security level (resilience) of solar photovoltaic (PV) infrastructures towards cyber-attacks.

The hybrid CNN–RNN model showed better detection performance toward ECGI, achieving an overall accuracy of 97.4% with AUC score of 0.98 as compared to those using other traditional machine-learning algorithms including SVM, RF and MLP [31].

Our findings are consistent with two recent studies from Lin *et al*. (2023) [5] and Yu *et al*. (2022) [10], who had approved that the hybrid deep models have a better detection accuracy in nonlinear and complex environments for instance smart grids.

The ability of the model to learn both spatial and temporal correlations in network data allowed it to distinguish multi-stage attacks such as FDI and DoS with high accuracy, as demonstrated by the confusion matrix (Figure 3).

5.2. Interpretation of Model Performance

The accuracy comparison (Figure 1) emphasizes the superior robustness of DL techniques when dealing with complex/ heterogeneous data as in PV networks.

Conventional ML models use handcrafted feature extraction and model training, but are not effective for learning dynamic attack behavior.

On the contrary, our CNN–RNN model autonomously captured hierarchical representations for robust detection across multiple threats.

The training and validation loss curves (Figure 2) showed that the models converged consistently with little over fitting, suggesting a good generalization performance and optimization ability.

This finding is consistent with Anwar, Sokolov and Sandberg (2022) [1], who stressed the importance of adaptive regularization to mitigate overfitting in the context of critical infrastructure security models.

In addition, the confusion matrix (figure 3) showed a high accuracy of classification across all attack classes with slight overlap between FDI and DoS attacks due to their close temporal and volumetric signatures (Harrou, 2023) [3].

The model's balanced recall and precision rates (>94%) indicate that it is robust in reducing both false positives and false negatives, which is of great importance for real-time decision making in PV control centers.

These characteristics were corroborated by ROC curve analysis (Figure 4), which demonstrated that the CNN–RNN combination yielded a far superior rate of true positive detections along with fewer false alarms in comparison to baseline techniques, enhancing both threat detection speed and reliability (Cooper *et al*., 2023) [2].

5.3. Contribution to Cyber Resilience

The concept of cyber resilience for energy systems relates to the capacity to anticipate, absorb, recover and adapt to cyber threats (NIST 2011) [8].

Developed model enhances this robustness in three main aspects:

Early Threat Detection: By having the model set at high accuracy and being out of false alarm, it saves both incident response time and potential operational downtime.

Adaptive learning: It has capability to keep re training itself for continuous feature extraction from traffic for new attack vectors (Munir, Shetty & Rawat 2023) [6].

Distributed defense: When combined with Edge AI deployment, support local detection and self-healing of inverter-level nodes according to CNN–RNN (Li *et al*., 2023) [4].

These results are consistent with NERC (2022) [7] suggestions on how to harden distributed energy resources (DERs) - the value of real-time, data-driven monitoring type systems.

Accordingly, this study advances the existing cybersecurity paradigms away from guarding and defending against attacks to utilizing AI-based models to implement resilience in a distributed solar energy system architecture.

5.4. Comparison with Prior Work

Related work in this area has been on general security research for smart-grid but not so much for solar-related case. For example, Aoufi, Elbrahmi and Boulmalf (2020) offered a general review of FDI countermeasure approaches without discussing deep learning integration.

The novelty of this study is that it models the time–space dependency and nonlinearity within PV data using a customized hybrid DL architecture.

Similarly, Lin *et al*. (2023) [5] utilized deep reinforcement learning for identification of FDI in power system while not dealing with IoT-based PV settings.

Through integrating CNNs for spatial pattern extraction and RNNs for temporal learning, this work provides an essential methodological bridge and customises deep learning methods to renewable-related cyber-physical systems.

Harrou (2023) [3] and Rahim *et al*., (2023) [9] also addressed the growing cyber threats in PV systems, e.g., inverter tampering and ill-intentioned configuration.

The results of our study support these concerns and propose an empirical defense strategy based on the validation under hybrid datasets.

Particularly, the detection performance of our proposed model exceeds 95% as reported in Yu *et al*. (2022) [10], which further proves the importance of combining real PV-SCADA data with benchmark dataset for better generalization.

5.5. Practical and Operational Implications

The operation advantages of AI-based intrusion detection in solar power conversion systems are as follows:

- **Self-Sufficient:** The CNN–RNN monitoring model is a self-sustained model which, once trained, needs no human involvement to monitor the inverter and communication system data.
- **Predictive Maintenance:** Anomalies could indicate hardware or driver errors, thus enabling preventive maintenance.
- **Minimized Downtime:** Early identification limits the time it takes to bring the system back up after a cyber event.
- **Scalable:** By employing Edge AI (i.e., edge-side intelligence) and federated learning, these models can be taken to various geographically-distributed PV units without exchanging data (Zhang *et al*., 2023) [11].

Such findings highlight the operational feasibility of low-latency, secure, environmentally friendly solar grid operations using deep learning.

5.6. Limitations and Future Research

Although these results are encouraging, we should acknowledge some limitations.

First, the hybrid model was partially based on widely accepted network intrusion datasets which may not reflect all operational features of solar SCADA traffic. In the future, solar-specific cybersecurity datasets should be developed with inverter telemetry data, weather fluctuations and power variations (Rahim *et al*., 2023) [9].

Second, although the model should scale well, computation complexity may be a concern for low-rate controllers. In the future, lightweight architectures like mobileNet or attention models based on transformer optimized for embedded PV devices should be investigated (Li *et al*., 2023) [4].

Finally, deep learning models perform as “black boxes,” which reduces interpretability. The utilization of Explainable AI (XAI) methods will contribute towards the transparency in operator confidence (Munir *et al*., 2023) [6].

Last but not least, the combination of AI systems with policy frameworks and grid codes (e.g., NISTIR 8259A, IEC 62351) is a future direction to facilitate regulatory compliance and holistic cyber governance.

5.7. Summary of Discussion

In particular, results solidify our claim that AI-enabled deep learning models (specifically so the CNN–RNN hybrid architecture) represent a game-changing solution for preserving solar infrastructures.

In this way, with the ability to effectively identify multi-class of attacks and stronger generalization power, the proposed model promotes both theoretical support ofbthe current cybersecurity in renewable energy system and its practical applications.

By fusing AI, edge computing and energy resilience concepts, we have an opportunity to carve out a vision for a new breed of self-defending adaptive solar grids that can deliver consistent secure and sustainable energy supply in the face of changing cyber security threats.

6. Conclusion

The combination of artificial intelligence (AI) and renewable energy systems is a momentous development in the study of safe, reliable, sustainable, and economically sound power generation. In this work, we proposed a deep learning–based intrusion detection framework for solar photovoltaic (PV) systems to mitigate the emerging cyber-physical security threats against smart-grid infrastructures. The hybrid CNN–RNN model obtained an accuracy of detection at an impressive 97.4% and AUC = 0.98, surpassing classical algorithms (SVM, RF, Multilayer perception). These results confirm the superior effectiveness of deep-learning models for detecting complex and evolving attack profiles on highly dynamics solar energy networks (Lin *et al*., 2023; Yu *et al*., 2022) [5, 10].

Three main contributions are delivered by the study to both academic and practical fields. First, the paper develops a domain-adapted hybrid DL model that can capture spatial and temporal dependencies in PV-SCADA data. This twint learning method allows the detection of cyber-attacks such as FDI, DoS and insider attack that most existing Security Systems are unable to detect (Harrou, 2023) [3]. Secondly, it is an evidence for the possibility of optimizing AI-based cybersecurity mechanisms to perform at edge space, leading to a real-time resiliency enhancement at inverter and microgrid levels (Li *et al*., 2023) [4]. Third, it fills an important gap in research validating deep learning models with the aid of a heterogeneous dataset which combines benchmark intrusion datasets (CIC-IDS2017, UNSW-NB15) and simulated PVSCADA communication flows, thus increasing the representativeness and reliability (Rahim *et al*., 2023) [9].

On a pragmatic level, these results indicate the revolutionary implementation of AI-based resilience frameworks for distributed renewable-energy networks. Deep learning architectures are capable of early threat detection and adaptive learning that can aid in utilities and operators preventing downtimes, increasing fault tolerance, and securing grid synchronization even during cyber events. They are also consistent with the advice provided by NERC (2022) [7] and NIST (2020) [8] of adopting proactive data driven cybersecurity strategies implemented in DERs. CNN–RNN framework, under consideration in this text, presents such a scalable approach which can seamlessly interface IoTAIs with the world of standards like IEC 62351 and NISTIR 8259A consolidating into standard-based and AI-driven grid security governance.

However, the work also points out important directions for future improvement. However, the model is partially built on generic network datasets, and has limited domain specificity. Construction of PV-oriented intrusion datasets with physical inverter telemetry and environmental data can notably enhance target detection precision and context confidence. Furthermore, lightweight AI architectures (e.g., MobileNet [16] or Transformerbased attention models) for real-time utilization on resource-constraint edge devices must be investigated in the future work. Note Added in Proof: It is also important to incorporate Explainable AI (XAI) techniques to improve transparency and trust from the operator, individuals making decisions should be able to understand and corroborate alerts generated by an AI system Munir, Shetty, & Rawat (2023) [6].

In summary, the work presented here supports deep learning as a viable and necessary route to securing future solar infrastructures. The combination method of CNN–RNN doesn't only improve diagnosis efficiency, it offers the key to build a self-repair, adaptive and intelligent electrical power system. With the transition of evolving global energy environments, embedding AI-based cybersecurity algorithms into renewable systems is essential to meet both technology innovation and sustainable energy security targets. The study thus paves the way for future multidisciplinary interplay among energy engineers, data scientists and policymakers towards developing resilient, intelligent and secure solar ecosystems.

7. References

1. Anwar M, Sokolov V, Sandberg H. Improving anomaly detection in SCADA network traffic using machine learning. Energy Inform. 2022;5(1):20. doi:10.1186/s42162-022-00252-1
2. Cooper A, Hill DJ, Bretas AS. Anomaly detection in power system state estimation: review and new directions. Energies. 2023;16(18):6678. doi:10.3390/en16186678
3. Harrou F. Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies. Front Energy Res. 2023;11:1274451. doi:10.3389/fenrg.2023.1274451
4. Li J, Zhou B, He X. Edge AI for renewable energy systems: opportunities and challenges. Renew Sustain Energy Rev. 2023;178:113260. doi:10.1016/j.rser.2023.113260
5. Lin X, Liu J, Wang H, Chen B, Yang J. False data injection attack and deep reinforcement learning-based detection in smart grids. Front Energy Res. 2023;11:1104989. doi:10.3389/fenrg.2023.1104989
6. Munir MS, Shetty S, Rawat DB. Trustworthy artificial intelligence framework for proactive detection and risk explanation of cyber attacks in smart grids. arXiv. 2023:2303.01145. Preprint.
7. North American Electric Reliability Corporation. Cybersecurity for distributed energy resources and DER aggregators. NERC; 2022.
8. National Institute of Standards and Technology. IoT device cybersecurity capability core baseline (NISTIR 8259A). NIST; 2020.
9. Rahim FA, Ahmad NA, Magalingam P, Jamil N, Cob ZC, Salahudin L. Cybersecurity vulnerabilities in smart grids with solar photovoltaic: a threat modelling and risk assessment approach. Int J Sustain Constr Eng Technol. 2023;14(3):210-20. doi:10.30880/IJSCET.2023.14.03.018
10. Yu T, *et al*. An advanced accurate intrusion detection system for smart grids. Front Energy Res. 2022;10:903370. doi:10.3389/fenrg.2022.903370
11. Zhang K, Lin X, Yang Q. Federated learning for cybersecurity in smart grids: opportunities and challenges. IEEE Internet Things J. 2023;10(4):3241-55. doi:10.1109/JIOT.2023.3234712
12. Dalal A. Data management using cloud computing. SSRN. 2023:5198760.
13. Mishra A. Harnessing big data for transforming supply chain management and demand forecasting.
14. Hegde P. Automated content creation in telecommunications. Jurnal Komputer Informasi dan Teknologi. 2021;1(2):20.
15. Tiwari A. Ethical AI governance in content systems. Int J Manag Perspect Soc Res. 2022;1(1&2):141-57.

16. Pimpale S. Optimization of complex dynamic DC microgrid using non-linear bang bang control. J Mech Civ Ind Eng. 2020;1(1):39-54.
17. Dalal A. Designing zero trust security models to protect distributed networks and minimize cyber risks. SSRN. 2021:5268092. doi:10.2139/ssrn.5268092
18. Mohammad A, Mahjabeen F. Promises and challenges of perovskite solar cells: a comprehensive review. BULLET J Multidisiplin Ilmu. 2023;2(5):1147-57.
19. Juba OO, Olumide AO, Ochieng JO, Aburo NA. Evaluating the impact of public policy on the adoption of community-based care for aged adults. Int J Mach Learn Res Cybersecurity AI. 2022;13(1):65-102.
20. Halimuzzaman M. Technology-driven healthcare and sustainable tourism. Bus Soc Sci. 2022;1(1):1-9.
21. Tiwari A. Artificial intelligence (AI's) impact on future of digital experience platform (DXPs). Voyage J Econ Bus Res. 2023;2(2):93-109.
22. Dalal A. Cybersecurity and privacy: balancing security and individual rights in the digital age. SSRN. 2020:5171893.
23. Lewechi FE. Zero trust framework for AI-enabled digital twin: integrating security, fairness, and compliance monitoring. Int J Multidiscip Res Growth Eval. 2023;4(6):1339-1347. doi:10.54660/IJMRGE.2023.4.6.1339-1347.
24. Lewechi F. Blockchain-orchestrated IAM for multi-cloud AI systems: identify federation with ethical controls. Int J Multidiscip Evolut Res. 2023;4(2):139–149. doi:10.54660/IJMER.2023.4.2.139-149.
25. Pimpale S. Impact of fast charging infrastructure on power electronics design. Int J Res Sci Manag. 2021;8(10):62-75.
26. Mishra A. Analysis of cyberattacks in US healthcare: review of risks, vulnerabilities, and recommendations. 2022.
27. Hegde P, Varughese RJ. Elevating customer support experience in telecom. Propel J Acad Res. 2023;3(2):193-211.
28. Dalal A. Leveraging cloud computing to accelerate digital transformation. SSRN. 2018:5268112. doi:10.2139/ssrn.5268112
29. Mohammad A, Mahjabeen F. Revolutionizing solar energy with AI-driven enhancements in photovoltaic technology. BULLET. 2023;2(4):1174-87.
30. Tiwari A. AI-driven content systems: innovation and early adoption. Propel J Acad Res. 2022;2(1):61-79.
31. Kacheru G. The future of cyber defence: predictive security with artificial intelligence. Int J Adv Res Basic Eng Sci Technol. 2021;7(12):46-55.
32. Dalal A. Exploring next-generation cybersecurity tools for advanced threat detection and incident response. SSRN. 2020:5424096.
33. Pimpale S. Hydrogen production methods: carbon emission comparison and future advancements. 2023.
34. Halimuzzaman M. Leadership, innovation, and policy in service industries. Bus Soc Sci. 2022;1(1):1-9.
35. Mishra A. Exploring ITIL and ITSM change management in highly regulated industries. 2021.
36. Dalal A. Maximizing business value through artificial intelligence and machine learning in SAP platforms. SSRN. 2019:5424315. doi:10.2139/ssrn.5424315
37. Hegde P. AI-driven data analytics: insights for telecom growth strategies. Int J Res Sci Manag. 2020;7(7):52-68.
38. Tiwari A. Generative AI in digital content creation, curation and automation. IJRSM. 2023;10(12):40-53.
39. Dalal A. Building comprehensive cybersecurity policies to protect sensitive data in the digital era. SSRN. 2023:5424094.
40. Pimpale S. Electric axle testing and validation: trade-off between computer-aided simulation and physical testing. 2022.
41. Mohammad A, Mahjabeen F. Revolutionizing solar energy: the impact of artificial intelligence on photovoltaic systems. IJMSA. 2023;2(3):591856.
42. Juba OO, Lawal O, David JI, Olumide BF. Developing and assessing care strategies for dementia patients. Int J Adv Eng Technol Innov. 2023;1(04):322-49.
43. Mishra A. Leveraging artificial intelligence to improve cybersecurity defences. SSRN. 2020:5422354.
44. Dalal A. Addressing challenges in cybersecurity implementation across diverse sectors. SSRN. 2022:5422294. doi:10.2139/ssrn.5422294
45. Hegde P, Varughese RJ. Predictive maintenance in telecom. J Mech Civ Ind Eng. 2022;3(3):102-18.
46. Pimpale S. Efficiency-driven and compact DC-DC converter designs. IJRSM. 2023;10(1):1-18.
47. Dalal A. Cyber threat intelligence: how to collect and analyse data. Int J Recent Innov Trends Comput Commun. 2020.
48. Tiwari A. Artificial intelligence's impact on DXPs. Voyage J Econ Bus Res. 2023.
49. Mohammad A, *et al*. The influence of hot point on MTU CB condition. J Renew Energy Electr Comput Eng. 2023;3(2):37-43.
50. Mishra A. Exploring barriers and strategies related to gender gaps in emerging technology. IJMRGE. 2021.
51. Dalal A. Cybersecurity and artificial intelligence: how AI is being used in cybersecurity. Turk J Comput Math Educ. 2018;9(3):1704-9.
52. Hegde P. AI-powered 5G networks: enhancing speed, efficiency, and connectivity. IJRSM. 2019;6(3):50-61.
53. Pimpale S. Safety-oriented redundancy management for power converters in AUTOSAR systems. 2022.
54. Dalal A. Exploring emerging trends in cloud computing and their impact on enterprise innovation. SSRN. 2017:5268114. doi:10.2139/ssrn.5268114
55. Tiwari A. Ethical AI governance in content systems. IJMPSR. 2023;1(1&2).
56. Mishra A. Energy efficient infrastructure green data centers: the new metrics for IT framework. 2022.
57. Halimuzzaman M, Gazi MAI, Rahman MS. Journal of Socio-Economic Research and Development-Bangladesh. 2013;10(5):1557-64.
58. Dalal A. Developing scalable applications through advanced serverless architectures in cloud ecosystems. SSRN. 2017:5423999.
59. Mohammad A, *et al*. Design and implementation of low cost MPPT solar charge controller. 2022.
60. Pimpale S. Comparative analysis of hydrogen fuel cell vehicle powertrain. 2020.
61. Hegde P. AI-driven data analytics: insights for telecom growth strategies. 2020.
62. Tiwari A. AI-driven content systems: innovation and early adoption. 2022.
63. Dalal A. Optimizing edge computing integration with cloud platforms. SSRN. 2015:5268128. doi:10.2139/ssrn.5268128

64. Mishra A. Agile coaching: effectiveness and best practices for successful Scrum adoption. 2020.
65. Dalal A. Building comprehensive cybersecurity policies. SSRN. 2023:5424094.
66. Tiwari A. Generative AI in digital content creation. 2023.
67. Halimuzzaman M. Loans and advances of commercial banks: Janata Bank Limited. CLEAR Int J Res Commer Manag. 2013;4(5).
68. Dalal A. Bridging operational gaps using cloud computing tools for seamless team collaboration. SSRN. 2016:5268126. doi:10.2139/ssrn.5268126
69. Pimpale S. Hydrogen production methods. 2023.
70. Mishra A. Analytical study of the FinTech industry's digital transformation. 2022.
71. Hegde P, Varughese RJ. Elevating customer support experience in telecom through AR. 2023.
72. Dalal A. Leveraging cloud computing to accelerate digital transformation. 2018.
73. Mohammad A, Mahjabeen F. Revolutionizing solar energy: the impact of AI on PV systems. 2023.
74. Tiwari A. Ethical AI governance in content systems. 2022.