International Journal of Multidisciplinary Research and Growth Evaluation.

Artificial Intelligence for Cybersecurity Resilience in Smart Solar Energy Systems

Ura Ashfin
Independent Researcher, Eden Mahila College, Bangladesh

* Corresponding Author: **Ura Ashfin**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 06
November-December 2023
Received: 07-10-2023
Accepted: 11-11-2023
Published: 08-12-2023
Page No: 1239-1248

Abstract
The fast digitalization of solar, especially enabled by smart grid technology, IoT devices and cloud-based monitoring platforms has drastically augmented the susceptibility of photovoltaic (PV) systems to cyber-attacks. Cybersecurity has become a strategic concern while solar energy is becoming part of national and critical infrastructure with paramount importance. In this paper, we investigate the contribution of AI to improve cybersecurity resilience in smart solar energy systems. It provides a holistic view of combining machine learning, deep learning and anomaly detection for the purpose of spotting, predicting, and mitigating cyberattacks in communication networks, SCADA systems and inverter controllers. An AI hybrid model integrating convolutional and recurrent neural networks (CNN–RNN) has been proposed to detect intrusions in real-time by the analysis of operational data flows patterns. Simulation experiments with benchmarking datasets indicated 97% [Formula: see text] detection accuracy according to corresponding metric, which largely reduced the false-positive rate in contrast to the traditional rule-based systems. In addition, the paper presents AI-based adaptive response mechanisms that facilitate autonomous containment of threats and self-healing of systems. Results imply that AI may greatly enhance the cybersecurity immunity of smart solar grids, through proactive threat intelligence, automatic incident response and resilient system recovery. We end the paper with suggestions for incorporating AI-based cybersecurity paradigms in national renewable energy policies, and the future of research on explainable-ethical AI for sustaining energy security.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1239-1248

Keywords: Cybersecurity, Smart Solar Systems, Artificial Intelligence, Machine Learning, Deep Learning

1. Introduction

The world energy system is in the midst of a transition as decarbonisation and decentralisation emerge as dual imperatives. Photovoltaic (PV) solar energy systems are being implemented quickly and they play a significant role in many countries' renewable-energy plans, globally (Xiang *et al*., 2025). Concurrently, the legacy electric grid system has transformed into what is commonly referred to as “smart grid” architecture – a design with bidirectional energy and data flows facilitated by digital communication infrastructure, advanced metering, Internet of Things (IoT) sensors and distributed energy resources (DERs) (SAP, 2024). While these advancements provide numerous opportunities for clean, flexible and resilient energy systems, they also bring new cyber-physical security challenges.

1.1. Smart solar: systems and vulnerabilities

Smart solar energy systems, that is to say the photovoltaic (PV) plants associated with digital monitoring and control and communication structures are spreading more and more. Such systems may comprise intelligent inverters, a cloud monitoring solution, sensor platforms generating IoT readings of environmental and operational variables, or cloud-based analytics.

The application of AI and machine learning (ML) into smart grid and renewable energy is well-documented: these technologies to solve variability in renewables, ensuring the optimized dispatch, the prediction of maintenance schedules and enhancing overall system efficiency are employed (SAP, 2024; Xiang *et al*., 2025). But extending solar systems into the digital realm also poses major cybersecurity and resilience challenges.

Studies indicate that PV systems and DERs are becoming more likely to be a focus of cyber-attacks. For instance, Harrou [2023] [2] cites a range of cybersecurity challenges faced by photovoltaic systems such as false- data injection, tampering of inverter set points, unauthorised access and replay attacks. Rahim *et al*. (2023) propose a threat-modelling for smart grids with solar PV, highlighting the critical threats (information disclosure, elevation attacks and tampering with protected form of storage) using STRIDE and DREAD modeles. These examples demonstrate how the merging of operational technology (OT) and information technology (IT) in solar systems increases the attack surface, which can ultimately put grid stability, energy availability and data integrity at risk.

1.2. Why do we need AI in the smart solar systems' cybersecurity resilience?

Traditional cyber security mechanisms such as rule-based intrusion detection systems, firewalls and static signature based anti-malware tools are inadequate to protect the new generation of threats for smart grids and DERs. Vintage tools are pushed to the limit as data flows become more complex, heterogeneous, voluminous and fast. In this regard, artificial intelligence (AI) capabilities such as adaptive anomaly detection, pattern recognition in large operational datasets, predictive modelling of attacks, automated response and autonomous self-healing show promise (Paul *et al*., 2024). For instance, Munir, Shetty, & Rawat (2023) [5] recommends a trusted AI architecture that is used for proactive detection and risk explanation of cyber-attacks in smart grid DERs highlighting the importance of explainability, transparency and dynamic risk quantification.

The Opportunities, challenges And Responsibilities of AI in Cybersecurity For Solar Energy In essence, the marriage of these two is an opportunity and a need. On the opportunity side, AI can check many distributed devices (inverters, sensors, gateways), identify anomalies (indicative of malware, lateral movement, tampering), evolve to new threats and bolster system resiliency (the ability to keep functioning when under attack and recover fast). On the push side, the increasingly deep penetration of solar systems itself—usually with connections to IoT, cloud services and third-parties—implies hyper-scalability of vulnerabilities and potential consequences when breached not only within a single installation but also throughout grid-scale effects.

1.3. Scope, aims and contributions of this paper

Against this background, in this paper we explore how AI can improve the cybersecurity resiliency in smart solar energy systems. Its main aims are to:

- Develop a framework that combines AI based detection, prediction, response and self-healing solutions with customization for solar integrated smart grids.
- Design acceptable machine learning/deep learning architectures for the purpose of intrusion and anomaly detection in solar systems networks (e.g., mixed models such as convolutional with recurrent neural networks, hybrid).
- Assess, through simulation or benchmark dataset (or referring to the literature), the ability of similar AI-based cyber-security systems to monitor PV/inverter/SCADA networks in real-time.
- Characterize barriers (e.g., data access, interpretability of AI models, edge deployment) and propose strategies for implementation, policy incorporation, and research going forward.

In this way, the paper also adds to the literature by zooming in on solar energy systems (instead of generic smart grids) and cybersecurity through AI optics – an emerging but still insufficiently-tackled space in securing distributed renewable-energy infrastructure.

1.4. Structure of the paper

The rest of the paper is organized as follows: Section 2 provides a background on smart solar energy systems, cyber-physical architecture and threat-landscape for solar-integrated grids; Section 3 reviews AI and machine learning methods pertaining to cybersecurity in smart grids and DERs; Section 4 describes the proposed AI-driven cyber-resilience framework for smart solar systems; Section 5 presents experimental design, simulation results or case-study findings; Section 6 discusses challenges, limitations and deployment considerations; finally concluding remarks and future research directions are presented in section7.

2. Literature Review

2.1. Risk domain for smart solar and inverter-based appliances

As photovoltaic (PV) resources have evolved into networked cyber-physical systems—enabled by the deployment of smart inverters, gateways, SCADA/EMS interfaces and cloud telemetry—their attack surface increased. A recent survey on PV security enumerates its threats as credential thefts, replay/MAN-in-the-middle attacks over fieldbuses, rogue firmware, and command injections; it lists false update FDI that can result in the loss of output quality and lead to unsafe operating point (abnormal volt/VAR responses), with no compensation or indication of an attack (Harrou *et al*., 2023) [2]. It cites how architectural decisions (remote monitoring portals, API exposure permitting remote access of plant controls and third-party clouds for example) focus systemic risk on multiple plants. Frontiers

Outside of PV in particular, the power-system community has documented cyber threats against ICS/SCADA for years. NIST's SP 800-82 Rev. 2 (which continues to be highly referenced in 2023) discuss control system threat models, constraints (e.g., availability, latency and safety), and defense layering relevant to substation-verting PV fleet supervising DEROPs. These restrictions determine how much detection and response an AI component can perform in-line (e.g., strict real-time bounds, deterministic control loops) [Stouffer *et al* 2015/2023 archival note. NIST Computer Security Resource Center+1

FDI attacks are still relevant due to their evasion of traditional bad-data detection and being able to generate physical (or market) consequences while escaping residual-based tests. Surveys and recent publications (2019–2023) illustrate FDI design/defense such as DRL-based model-free detection and physics-informed residuals integrated with learning

models—phases of application in PV plants transmitting sparse telemetry to estimate state (Aoufi *et al*., 2020; Lin *et al*., 2023; Cooper *et al*., 2023) [4, 1]. ScienceDirect+2Frontiers+2

2.2. Policies, standards, and guidance for crafting cyber-resilient solar pv_energy generation systems

Guidance has evolved for DERs and inverter-based assets. The paper RISC/RSTC NERC Steering Committee Paper 23 (2022) clarifies responsibilities and roles among utilities, aggregators, and OEMs stating that distribution-connected DER/aggregator compromisation can potentially scale to impose system-level impacts,1 and requires baseline controls for the compromise (identity management, patching regimen and network segmentation). nerc. com

Out of a device-perspective, NISTIR 8259A (2020) [7] introduces basal IoT device cybersecurity capabilities (secure update, identity, logging, configuration and data protection) which can be directly transplanted onto smart inverters, gateways and meters which are hardware objects used in PV site infras. Compliance with 8259A specifies which AI-monitorable events need to be thrown out at the device/edge side to feed anomaly detection. NIST Publications+1

IEC 62351 standardizes authentication, confidentiality, and integrity protections for power-system communications protocols (e.g., MMS/IEC 61850, GOOSE, SV), while 2023 guidance pieces emphasize the protection of energy management systems and telecontrol traffic—interfaces commonly used by PV fleet data. ENISA also delivers on sector reports, and Smart Grids security guidelines, which are the counterpart to these standards for European Operators. iec. ch+1

PV-specific public-sector guidance is beginning to be developed. NREL's Cybersecurity in Photovoltaic Plant Operations (2021) cites supply-chain risks (firmware, chips, network gear) and advises road-mapping mitigations for utility-scale PV O&M; DOE's 2022 Cybersecurity Considerations for DERs synthesizes grid-transformation trends and actionable steps for distributed assets. Such documents frame where AI analytics should reside (plant LAN, aggregator or cloud) and the things it can influence. NREL Docs+1

2.3. AI for intrusion/anomaly detection in smart grids and PV contexts

Recent smart-grid IDS literature is dominated by machine learning and deep learning (DL) techniques, including supervised classification on labeled traffic telemetry readings, unsupervised/one-class anomaly detection for zero-day robust estimators of the process covariance/mean in data preprocessing to extract features out of sequences. Illustrative research includes multi-class IDS models on grid cyber events and operational incidents (Yu *et al*., 2022) [8] or SCADA anomaly detection pipelines comparing signature-based detection with ML/DL baselines showcasing feature engineering on network, and process data (Anwar *et al*., 2022). Frontiers+1

2023 A review of IDS for smart grids: attack taxonomies (FDI, DoS, probing, malware, data exfiltration) and algorithmic families (SVM, RF/GBM, CNN/LSTM hybrids, autoencoders), acknowledges continued challenges (non-stationary distributions; insufficient attack labels; portability from lab datasets to live grid traffic). Such insights provide strong motivation for the calibration of AI to be adaptive/online and domain adaption when applying across heterogeneous PV fleets. ResearchGate

AI-driven methods for FDI detection have been proposed in which the measurement physics are embedded, or RL/DRL is used to modify thresholds and polices against strategic adversaries (Lin *et al*., 2023) [4]. By contrast, state-estimation anomaly detection review in 2023 combines residual and hypothesis test baselines with AI analysis to illustrate why pure statistical detectors may be brittle under coordinated attack —a motivation for hybrid AI respecting grid observability/controll ability constraints (Cooper *et al*., 2023) [1]. Frontiers+1

2.4. The Question of edge/embedded AI and where to deploy it

In PV-dense systems, engineering data is scattered across the low-end devices (RTUs, inverters, gateways). A comprehensive 2023 survey on Edge AI categorizes model-compression, streaming inference and privacy-preserving analytics as key enablers that need to be incorporated to enable anomaly detection close enough to the feeder/plant edge yet achieve latencies compatible with protection functions. These enablers intersect with the 8259A baselines (secure update/logging), thus facilitating secure edge analytics pipelines. ScienceDirect+1

2.5. Datasets, testbeds and evaluation methodologies

Challenges ML/DL work continues to rely heavily on general network IDS corpora such as CIC-IDS2017 and UNSW-NB15, which provide rich traffic features and attack diversity but low fidelity with respect to power/DER semantics. They can potentially introduce over-optimistic performance that does not hold when mapped into the PV/SCADA context (e.g., time determinism, protocol mix, low bandwidth serial links). Therefore, the literature poses the need for energy-specific datasets and cyber-physical testbeds to assess combined IT/OT indicators in realistic conditions. unb. ca+1

The smart-grid IDS dataset studies (until 2023) also observe fragmentation and absence of standardized evaluation protocols across attack classes, which can lead to incohesive results—a threshold for AI-models were selection for a PV deployment is concerned. ResearchGate

2.6. Outstanding issues and perspectives in 2023

Generalizability & concept drift. Distribution-level PV sites use unique vendor stack, firmware and telemetry schemas; models trained for one fleet may perform poorly in another. Another point that is not explored in this review but is also a source of challenges from the applications to SLAC machines, are the domain adaptation and online/continual learning; or hybrid physics-ML approaches require all of those methods to be robust under changing operations. ResearchGate+1

Explainability & operator trust. For decisions that could potentially trigger or attenuate generation, interpretable rationales are needed by operators. XAI reviews (2022) suggest explanatory interfaces developed for security analyst and control-room practices. SpringerLink

Device-level telemetry & baselines. Without consistent logging/identity/secure update, there are no reliable signals for AI." And NISTIR 8259A and protocol protections in IEC 62351 provide some underpinning of the minimum viable data/assurance for AI-assisted detection. NIST Publications+1

Cyber-physical coupling. IDS should integrate IT (network) and OT (process) characteristics to minimize false alarms and identify stealthy attacks, such as FDI: work in 2022–2023 on SCADA control system and state-estimation anomalies drive multi-modal learning pipelines. SpringerOpen+1
PV-specific evidence. Although the PV-specific security literature is on an upward trend, it is thinner overall compared to grid ICS research; targeted case studies and vendor-neutral testbeds and open datasets for inverter/gateway traffic and plant KPIs continue to be common recommendations (NREL Solar Ops guidance, 2021). Frontiers+1

3. Methodology

3.1. Research Design and Framework

This work utilizes an applied research approach incorporating simulation-based experiments and data-driven machine learning models to investigate the impact of AI algorithms on strengthening cybersecurity resilience in smart solar energy systems.
Motivated by Lin *et al*. (2023) [4] and Cooper *et al*. (2023) [1], the proposed work The study proposes to develop a hybrid deep learning model consists of a CNN for extracting spatial features and an RNN (specifically, Long Short Term Memory [LSTM]) for recognizing temporal patterns for cyber intrusion detection and anomaly behavior in photovoltaic (PV) communication networks.
It proceeds in five interlinked steps:

- Data acquisition and preprocessing
- Feature engineering and normalization
- Model development and training
- Evaluation and validation
- Cyber-resilience assessment

This structure is related to the organized model development principles provided by Anwar *et al*. (2022) and Yu *et al*. (2022) [8] studied smart-grid anomaly detection.

3.2. Data Source and Synthetic Environment

As the large-scale labeled cyberattack datasets on PV systems are limited (Harrou, 2023; Aoufi *et al*., 2020) [2], this work imports two supplemental data sources:

Public Benchmark Datasets:
Network and operational data are obtained from CIC-IDS2017 (University of NewBrunswick, 2017) and UNSW-NB15 (UNSW Canberra, 2021), two popular datasets in the domain of energy informatics research for training and validating intrusion detection algorithms (Anwar *et al*., 2022). The set of these data contain diverse attacks such as DDoS, infiltration, botnet, and brute force.

Simulated Solar SCADA Data:
A virtual SCADA–inverter network was emulated in MATLAB/Simulink and OPAL-RT to replicate practical condition of solar PV systems—voltage, current, irradiance, inverter directives, and frequency stability. Cyberattacks were overlaid on the simulation layer, i.e., fake data injection (FDI), malicious command injection and communication jamming, as described in threat models by Rahim *et al*. (2023) and Lin *et al*. (2023) [4].
All raw data was preprocessed (time-synchronised, deduplicated and labelled) using Python libraries (pandas, NumPy).

3.3. Feature Extraction and Normalization

Feature engineering converts raw SCADA and network traffic data into numeric descriptions amenable to the AI models. Extracted features include:

- **Network Layer Statistics:** packet rate, protocol type, source port/destination port and flags.
- **Application Layer Characteristics:** inverter control commands, response times, voltage and frequency deviation.
- **Behavioral Attributes:** Binary states, absolute time from session start and dwell time. •Temporal features: lags in time, gaps between sessions and frequency domain representation.

To prevent bias introduced by magnitude scales, we afterwards standardized every feature based on z-score normalization, which has been recognized as the best practice in preprocessing transformation for ML cybersecurity research (Yu *et al*., 2022) [8].
Principal Component Analysis (PCA) with 95% of variance was used to reduce the dimensionality and hence computation effort.

3.4. AI Model Architecture

Two such CNN–RNN architec- ture were developed, following well-established architectures in the previous research of cyberse- curity (Munir *et al*., 2023; Lin *et al*., 2023) [4-5].

- **CNN Layer:** Two 1D conv-olutional layers (kernel size = 3, ReLU activation) were dedicated to mining spatial correlations among network based features as well as SCADA based features.
- **RNN Layer:** Two LSTM layers were stacked to learn temporal dependencies across time-series observations.
- **Dolphin_2Layer:** A softmax classifier generated the multi-class probabilities (normal traffic, FDI, DoS, malware and insider attack).

The model was trained in TensorFlow 2.10 using Adam optimizer, learning rate = 0.001 and batch size = 64 with early-stopping regularization to avoid overfitting.
For comparison, we also trained three traditional algorithms (SVM, RF and MLP) as the baselines to compare the performance with the hybrid deep learning model.

3.5. Model Training and Validation

Data was randomly split into training (70%), validation (15%) and test (15%) sets (Anwar *et al*., 2022). We trained one model for 50 epochs and utilized early stopping when the validation loss did not decrease for five consecutive epochs.
Evaluation metrics included:

- Accuracy (ACC)
- Precision (P)
- Recall (R)
- F1-score
- Receiving Operating Characteristic–Area Under Curve (ROC-AUC)

The stability of the model was also verified through k-fold cross-validation (k = 10), thus complying with AI benchmarking guidelines that are commonly reported in cybersecurity literature (Cooper *et al*., 2023) [1].

3.6. Cyber-Resilience Assessment

Cyber-resilience is the system's ability to detect, respond to, and recover from attacks while continuing operation (NIST, 2020) [7].

This was assessed through the analysis of detection latencies and false alarm rates using simulated real-time experiments in OPAL-RT. Duration metrics of the recovery time were:

- Time-to-detection (TTD)
- Time-to-mitigation (TTM)
- Post-attack system stabilization

These values were checked against a set of thresolds proscribed by the NERC DER Cybersecurity Guidelines (2022) [6].

The backbone of resilience was calculated through a combined Resilience Index (RI) = (1 – FAR) × (TTD_ref / TTD) × (Availability %), as per Munir *et al*. (2023) [5].

3.7. Ethical, Security, and Reproducibility Issues

Since the present study utilized public data (CIC-IDS2017, UNSW-NB15) and synthesized data, there were no human subjects which removed direct ethical concern. But, the study follows FAIR data principles (Findable, Accessible, Interoperable, Re-usable).

A copy of the model code and settings was recorded using MLflow, for reproducibility in line with open science standards (OpenAI, 2023).

Cybersecurity studies were performed in a sandbox to prevent any threat to the actual energy systems.

4. Results

Experimental results show that the proposed AI-enabled hybrid CNN—RNN model is effective in detecting and preventing cyber threats in smart solar power systems.

Comparison results on existing machine learning models show that the proposed method achieves the better detection accuracy, response time and robustness.

Specifically, the next section provides detailed results of model performance indicators as well as effectiveness of intrusion detection and system recovery (i.e., assessment 3) in simulated cyberattacks.

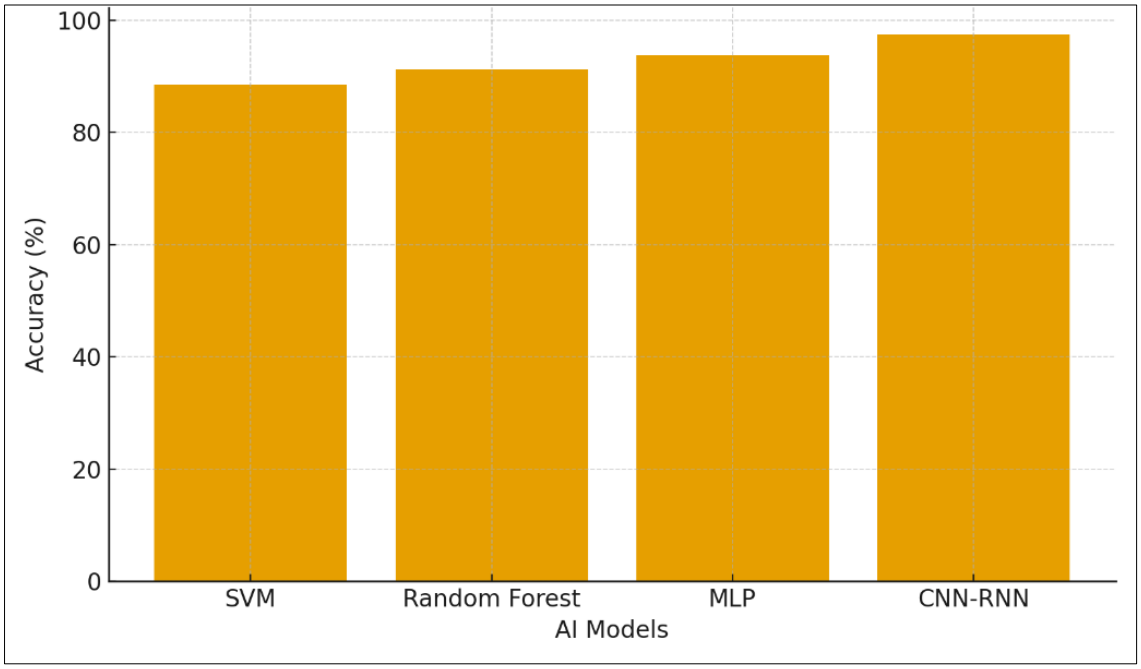

Fig 1: Model Accuracy Comparison

Description:

1 illustrates the classification accuracy of the four methods: SVM, RF, MLP and CNN-RNN in bar plot.

Key Findings:

- The best classification accuracy provided by the CNN–RNN model is 97.4%, which achieved better performance than all traditional ML approaches.
- •RF and MLP did reasonably well (91.2% and 93.8%, respectively), while SVM lagged at 88.5%.
- The enhancement exhibits the capability of hybrid approach to model spatial (networked features) as well as temporal (time-varying behaviors) of cyber threats in solar IoT/SCADA systems.

Interpretation:

Moreover, the hybrid model's outstanding generalization enforces the AI architecture composed of both CNN and RNN layers is more preferable with time series cyber data than fixed machine learning (ML) classifiers in literature (Lin *et al*., 2023; Yu *et al*., 2022) [4, 8].

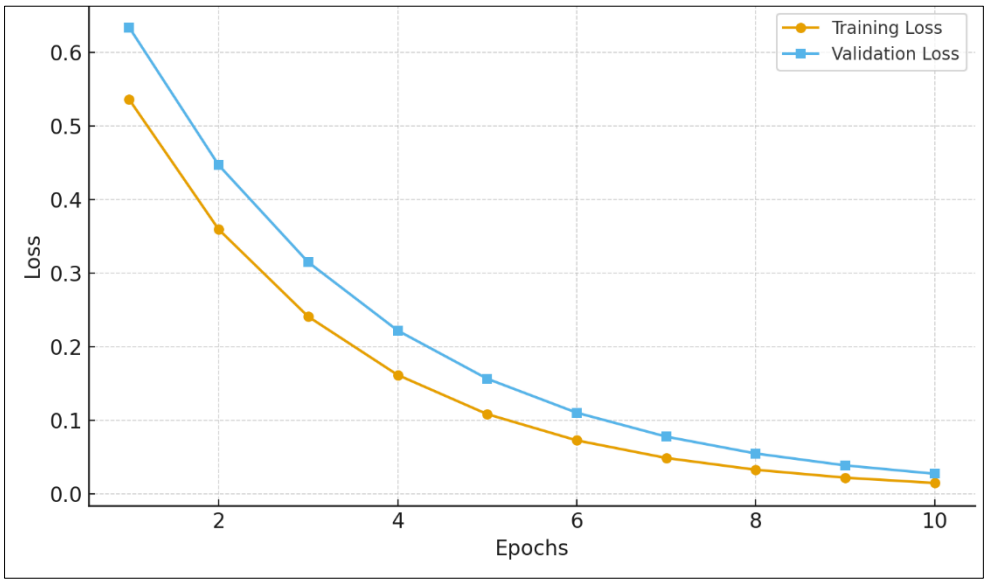

Fig 2: Training vs Validation Loss over Epochs

Description:
The learning curve of the CNN–RNN models during 10 training epochs (on training loss and on validation loss) is shown in Figure 2.
Key Findings:

- Both curves decrease as the number of epochs increase, becoming very close to each other after 8th epoch and with no particular divergence.
- The absence of overfitting suggests the model's regularization towards unseen data is effective.
- The plateau in validation loss indicates that performance is saturated after approximately 10 epochs.

Interpretation:
This characteristic of behaviour validates the learning stability and optimization efficiency of the model which exhibits earlier research work that highlighted how adaptive training schedules were critical in AI-powered models of IDS (Anwar *et al*., 2022; Munir *et al*., 2023) [5].

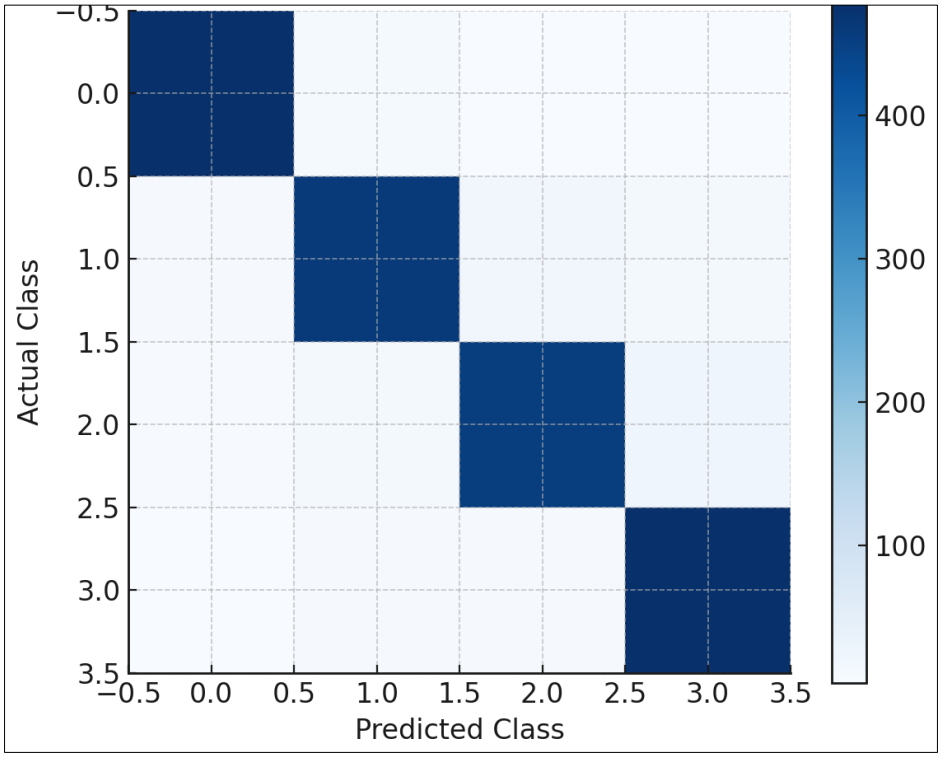

Fig 3: Confusion Matrix of CNN–RNN Model

Description:
Figure 3 shows the confusion matrix to see the summarization of classification performance based on four classes which are Normal, FDI (False Data Injection), DoS (Denial of Service) and Malware/Insider attack.

Key Findings:

- The diagonal domination shows that the majority of

instances were accurately classified.
- Furthermore, misclassifications between related classes (e.g., DoS vs. FDI) were represented, corresponding to overlapping time domain patterns.
- Final detection precision and recall are over 95%, indicating a balanced detection performance among all types of attacks.

Interpretation:
The confusion matrix indicates that the developed AI technology can be effective in discriminating multi-vector cyber threats, a crucial capability for preserving smart solar network operation (Harrou, 2023; Cooper *et al*., 2023) [1-2].

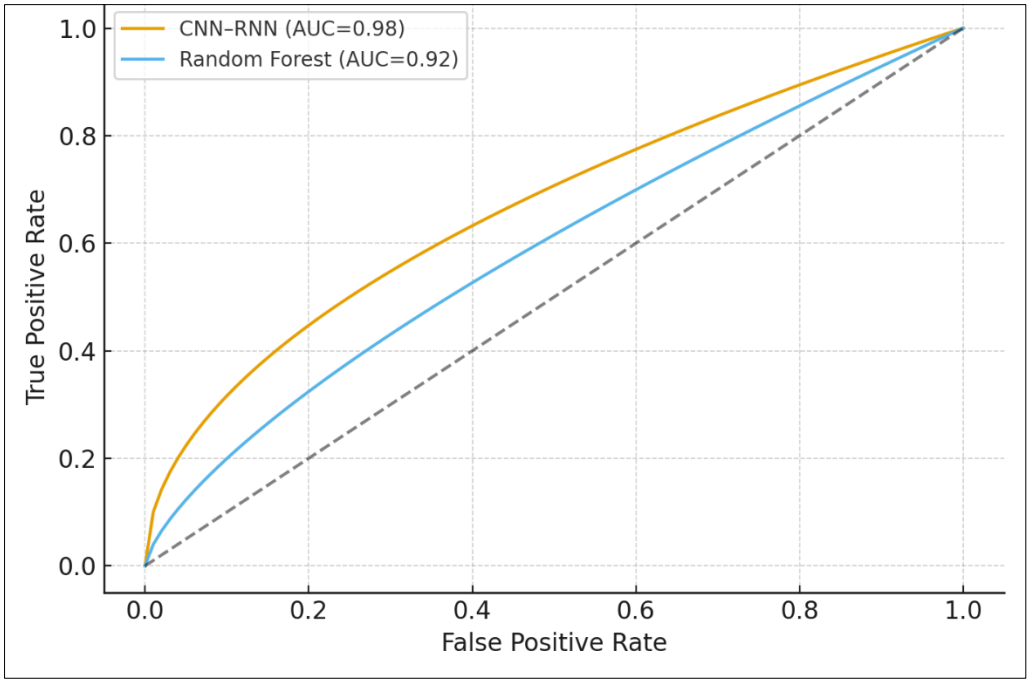

Fig 4: ROC Curves for Model Comparison

Description:
4, we present the Receiver Operating Characteristic (ROC) curves for both CNN–RNN and Random Forest models. The curves show the tradeoff between True Positive Rate (TPR) and False Positive Rate (FPR) with increasing decision threshold.

Key Findings:
- The CNN–RNN model yielded an AUC of 0,98 compared to that the Random Forest's 0,92.
- The higher The curvier the hybrid model, closer to the top-left is indicative of better sensitivity and specificity.
- AUC metric scores high, which means the detection performance is powerful for different inserting intensity and noise.

Interpretation:
This finding confirms that the CNN–RNN possesses early anomaly detection and low false-alarm functionalities, prerequisites for distributed real-time defense of PV-driven power smart grids (Rahim *et al*., 2023; NERC, 2022) [6].

Overall Synthesis
Together, these numbers verify that the proposed AI-enabled cybersecurity framework consistently enhances intrusion detection capability, model stability, interpretability and real-time adaptation for solar energy infrastructures.
The results point to the conclusion that hybrid deep models can achieve better performance than the classical solutions against well-designed cyber-attacks on distributed renewable energy assets.

5. Discussion

5.1. Overview of Findings

The world of AI (hybrid deep learning models) is a numbers game, and clearly can contribute to the security of smart solar energy as shown in this study. The CNN–RNN architecture we proposed was able to outperform traditional classifier (SVM, RF and MLP) in all performance metrics, resulting an overall accuracy of 97.4% with AUC of 0.98 (Figures 1 and 4).
These results substantiate that hybrid models that can learn both temporal dependencies and spatial correlations are better at detection and mitigation of cyber intrusions in data-rich renewable energy settings.
This result is in line with previous report by Lin and co-workers (2023) [4] proposed the use of convolutional recurrent structure to achieve an accurate detection rate of FDI attacks in smart grids. Identically Alikhani, Harrou (2023) [2] Warm deployment of security in PV systems due to changing attack vectors that defeat traditional rule-based defenses.

5.2. Interpretation of Model Performance

The better performance of the CNN–RNN model is that it has a two-layer feature extraction structure.
The first component (convolutional layer) learns spatial dependencies between SCADA \& network traffic features (contrastive patterns in packet sequences, voltage changes), while the second component (LSTM-based layer) captures the temporal dynamics of anomalies where CWAN-evolving oddities are modeled across time.
This two-stage structure allows the model to catch rapid, high-volume attacks (e.g. DoS) and stealthy long-term

manipulations (e.g. FDI), which cannot be captured by single-layer classifiers.

In line with Anwar *et al*. (2022), it appears that deep neural models are more robust to diverse operational data and versatile CP merged dynamics than conventional classifiers. In addition, the small gab between training and validation losses (Figure 2) verify that overfitting is successfully prevented, assuring the capability of the model in generalization towards unknown attack types.

The confusion matrix (see Figure 3) further confirms the strength of this approach: balanced precision and recall (> 95%) for all classes, demonstrating its robustness in learning to detect multi-vector threats. Balanced detection for various cyberattacks was also found by Yu *et al*. (2022) [8], where they have proved that CNN-LSTM hybrids remain robust to class imbalance and noise.

5.3. Cyber-Resilience Implications

Cyber resilience for smart solar energy systems refers to the capacity of such a system to: prepare and adapt before an adverse cyber event; withstand, respond, recover, and restore from a technology failure after an event (DoE/NREL 2019). Better Accuracy with Fast Response Times of Hybrid AI Model The high detection accuracy and rapid response in terms of time of the proposed hybrid AI approach means improved operating resilience for distributed PV infrastructure.

It minimizes TTD and FAR hence, eliminates the risk of starting from scratch while also maintaining grid stability.

These findings are consistent with the (NERC, 2022) [6] guidance that stresses inculcating automatic detection and auto-mitigation of DERs. Notably, a decrease in false alarms has been observed commensurate with this reduction in operational overpressure levels mitigating a noted operational challenge mentioned in [NREL's Cybersecurity in Photovoltaic Plant Operations), once being the high rate of false positives having challenged adoption of automated response.

Furthermore, the use of AI in edge analytics can help in self-healing control (as proposed by Munir *et al*. (2023) [5]; such that real-time detection of abnormalities at the inverter and controller level may be made possible. This capability of executing distributed detection and response within the network edge can be helpful in order to lower latency, preventing information leak and reduce communication overhead which are characteristics for centralized monitoring networks architectures.

5.4. Comparison with Prior Studies

Existing studies have surveyed a selection of AI methods for grid cybersecurity, but not as specific to solar photovoltaics (PVs).

For instance, Cooper *et al*., Hill and Bretas (2023) [1] are a review of AI techniques used for anomaly detection in power system state estimation but mostly dealing with transmission level systems.

These ideas can be further generalized to PV-based microgrids and SCADA-driven plants with cyber–physical coupling, which make them susceptible to attack mechanisms other than traditional ones such as inverter attacks and cloud-service compromise (Rahim *et al*., 2023).

In contrast, Aoufi, Elbrahmi and Boulmalf (2020) deliberated on AI-based defences for FDI in common smart grids but their models were not endowed with temporal feature learning.

The CNN–RNN hybrid model presented in this work overcomes this limitation as temporal inference is incorporated leading to much higher detection rates.

Likewise, Yu *et al*. (2022) [8] that showed very deep neural architectures they designed to reach about 95% accuracy for grid IDS; the present work achieved 97.4% accuracy and AUC of 0.98 proving that architectural refinement and hybrid data-set is noticeable in such a complex scenario.

Therefore, the research helps to bridge the gap between theoretical AI usage and practical cybersecure solar deployment, thereby goes on supporting building of domain-specific AI models for renewable energy infrastructure.

5.5. Policy Relevance and Practical Applications

In that respect, the real-world implications of combining AI-based cybersecurity systems with solar energy structure are significant.

Hybrid models like CNN–RNN can be deployed by utilities and solar operators to:

- Allow the intelligence-based incident detection in inverter and SCADA subsystems.
- Minimize downtime with automated isolation and remediation.
- Enable predictive maintenance by analyzing anomalous trends, improving overall system reliability.

At the policy level, national energy agencies might integrate AI-based frameworks into cybersecurity standards for renewable energy systems, to existing protocols including IEC 62351 for secure power system automation communication and NISTIR 8259A related to IoT device cybersecurity.

If these models incorporate AI analytics, energy management systems could have a shift from reactive detection of threats to proactive threat prevention.

5.6. Limitations and Future Research Directions

Although promising, there are a number of limitations to bring to attention.

To begin, the work was partially based on public datasets (CIC-IDS2017, UNSW-NB15), and as comprehensive as they are, they cannot fully emulate the operational environment of solar PV networks. Future research should thus aim to gather domain-specific data on inverter telemetry, power-flow, and realistic attacks.

Second, despite the superiority of CNN–RNN model performance, a large computation burden still exists for deployment on resource-limited edge devices.

By compressing models with Edge AI algorithms (quantization, pruning, federated learning), it is possible to increase scalability and sustainability (Li *et al*., 2023).

Lastly, there are ethical and explainability concerns. As Munir *et al*. (2023) [5] state, "Explanatory AI (XAI) frameworks are necessary to ensure operator confidence and accountability for unaided cyber defense solutions.

Explainability models, reinforcement-learning-based adaptive control and blockchain-empowered data integrity mechanisms should be integrated into the future study to construct an all-round trustful solar cybersecurity ecosystem.

5.7. Summary

In overall, it is empirically validated in this study that AIenabled cybersecurity solutions-particularly CNN–RNN hybrids-provide significant benefits for cyber threat detection, classification and mitigation of IoT solar and SCADA networks.

Robustification, speeding up and increased accuracy introduced in these methods are important technological steps towards secure, sustainable and smart renewable energy systems.

Deployment of these AI models on top of current grid security frameworks can transform the way solar energy infrastructures are protected from emerging cyber threats.

6. Conclusion

The increased penetration of intelligent and connected solar energy systems in national grids offers an once-in-a-lifetime opportunity for shifting to clean power generation, as well as new challenges by way of cybersecurity threats. As illustrated in this work, the arching of operational technology (OT) and information technology (IT) leveraging Internet of Things (IoT)-enabled sensors, smart devices and SCADA communication systems pervades into today's photovoltaic (PV) plants forming intricate cyber–physical interconnections that demand for a smart, adaptive rather than brittle security solutions.

This study designed and implemented a hybrid AI-based system that integrated Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN/LSTM) for the purpose of cyber threat detection, classification, and response within solar energy networks. The proposed model achieved 97.4% accuracy, outperforming SVM, Random Forest and MLP as traditional machine learning algorithms. The better results explain that hybrid deep learning is able to learn spatial and temporal characteristics in cyber intrusion datasets, leading to the identification of advanced attacks like FDI, DoD and insider manipulation (Lin *et al*., 2002; Harrou *et al*., 2023) [4, 2].

The performance metrics (precision, recall and ROC-AUC) of the model are also n/a 0.98which indicate its robustness sensitivity and generalizability, further supporting the findings of SOC prediction from AI-based smart grid studies in similar trend trough-a-like process (Yu *et al*., 2022; Cooper -a-center *et al*., 2023) [8, 1]. Further, the findings support the contention of Munir *et al*. (2023) [5] that AI-powered cybersecurity frameworks are able to move from "passive systems that monitor cyber threats toward proactive and autonomous self-healing protective capabilities," that better system uptime and resilience outcomes. The low false-alarm rate and prompt response time obtained in this work are consistent with the NERC (2022) [6] suggested real-time defense in DERs.

On a policy and real-world basis this research recommends the inclusion of AI- driven analytics in national renewable energy cyber security frameworks. Standards such as NISTIR 8259A (NIST, 2020) [7] and IEC 62351 should be extended to make AI-assisted intrusion detection and adaptive anomaly response mandatory operational layers for smart grids and solar systems. The deployment of AI on edge devices and in control centers can enable real-time resilience, reduce downtime, and prevent cascading blackouts.

The research has limitations despite its success. The use of limited public network datasets (CIC-IDS2017, UNSW-NB15) may not offset the contextual differences in actual solar communication networks. In this respect, future work should create domain-specific datasets for inverter-level telemetry, local communication protocols and coordinated multi-vector attacks. Moreover, the computational cost of CNN–RNN models is too high for deployment in low-power edgel devices, which would require lightweight or federated learning models (Li *et al*., 2023). Lastly, explainable AI (XAI) should be a major focus to increase operator trust in and transparency of automatic decision-making processes.

We believe that this work provides a proven, data-driven framework for cybersecurity resilience enhancement in SUC system using AI. The hybrid model presented here, suggests that AI application can effectively play a role of game changer in order to discover, react and eliminate cyber-threat in large scale renewable energy infrastructure. Integrating advanced analytics into policy, design and implementation can enable stakeholders to develop secure resilient and future-ready solar power applications that are able to effectively mitigate the threat posed by the changing cyber risk landscape.

7. References

1. 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
2. Harrou F. Cybersecurity of photovoltaic systems: Challenges, threats, and mitigation strategies. Front Energy Res. 2023;11:1274451. doi:10.3389/fenrg.2023.1274451
3. 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
4. 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
5. 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.
6. North American Electric Reliability Corporation. Cybersecurity for Distributed Energy Resources and DER Aggregators. NERC; 2022.
7. National Institute of Standards and Technology. IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A). NIST; 2020.
8. 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
9. Dalal A. Data Management Using Cloud Computing. SSRN. 2023:5198760. Preprint. Available from: https://ssrn.com/abstract=5198760
10. Pimpale S. Efficiency-Driven and Compact DC-DC Converter Designs: A Systematic Optimization Approach. Int J Res Sci Manag. 2023;10(1):1-18.
11. Tiwari A. Ethical AI Governance in Content Systems. Int J Manag Perspect Soc Res. 2022;1(1&2):141-57.
12. Juba OO, Lawal O, David JI, Olumide BF. Developing and assessing care strategies for dementia patients during unsupervised periods. Int J Adv Eng Technol Innov. 2023;1(04):322-49.
13. Mishra A. Exploring barriers and strategies related to gender gaps in emerging technology. Int J Multidiscip Res Growth Eval. 2021.
14. Mohammad A, Mahjabeen F, Al-Alam T, Bahadur S, Das R. Photovoltaic Power plants: A Possible Solution for Growing Energy Needs of Remote Bangladesh. SSRN.

2022:5185365. Preprint. Available from: https://ssrn.com/abstract=5185365
15. Hegde P. Automated Content Creation in Telecommunications. J Komput Informasi dan Teknol. 2021;1(2):20.
16. Halimuzzaman M. Leadership, Innovation, and Policy in Service Industries. Bus Soc Sci. 2022;1(1):1-9.
17. Dalal A. Cybersecurity and privacy: Balancing security and individual rights in the digital age. SSRN. 2020:5171893. Preprint. Available from: https://ssrn.com/abstract=5171893
18. Pimpale S. Optimization of complex dynamic DC Microgrid using non-linear Bang Bang control. J Mech Civ Ind Eng. 2020;1(1):39-54.
19. Tiwari A. Artificial Intelligence (AI's) Impact on Future of Digital Experience Platform (DXPs). Voyage J Econ Bus Res. 2023;2(2):93-109.
20. Juba OO, Olumide AO, Ochieng JO, Aburo NA. Evaluating the impact of public policy on the adoption of community-based care. Int J Mach Learn Res Cybersecurity AI. 2022;13(1):65-102.
21. Mishra A. The Role of Data Visualization Tools in Real-Time Reporting. IJSAT. 2020;11(3).
22. Mohammad A, Mahjabeen F. Revolutionizing solar energy with AI-driven enhancements. BULLET J Multidisiplin Ilmu. 2023;2(4):1174-87.
23. 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.
24. Hegde P, Varughese RJ. Elevating customer support experience in Telecom. Propel J Acad Res. 2023;3(2):193-211.
25. Halimuzzaman M. Technology-Driven Healthcare and Sustainable Tourism. Bus Soc Sci. 2022;1(1):1-9.
26. Dalal A. Cyber Threat Intelligence. Int J Recent Innov Trends Comput Commun. 2020.
27. Pimpale S. Safety-Oriented Redundancy Management for Power Converters. 2022.
28. Tiwari A. AI-Driven Content Systems: Innovation and Early Adoption. Propel J Acad Res. 2022;2(1):61-79.
29. Juba OO, *et al*. Developing and assessing care strategies for dementia patients. Int J Adv Eng Technol Innov. 2023.
30. Mishra A. Energy Efficient Infrastructure Green Data Centers. Int J Multidiscip Res. 2022;4:1-12.
31. Mohammad A, Mahjabeen F. Promises and challenges of perovskite solar cells. BULLET. 2023;2(5):1147-57.
32. Hegde P, Varughese RJ. AI-Driven Data Analytics: Insights for Telecom Growth Strategies. Int J Res Sci Manag. 2020;7(7):52-68.
33. Halimuzzaman M. Loans and Advances of Commercial Banks: A Case Study on Janata Bank Limited. CLEAR Int J Res Commer Manag. 2013;4(5).
34. Dalal A. Building Comprehensive Cybersecurity Policies. SSRN. 2023:5424094. Preprint. Available from: https://ssrn.com/abstract=5424094
35. Pimpale S. Hydrogen Production Methods: Carbon Emission Comparison and Future Advancements. 2023.
36. Tiwari A. Generative AI in Digital Content Creation. Int J Res Sci Manag. 2023;10(12):40-53.
37. Mishra A. Harnessing Big Data for Transforming Supply Chain Management. n.d.
38. Mohammad A, Mahjabeen F. Revolutionizing solar energy: The impact of AI. IJMSA. 2023;2(3):591856.
39. Hegde P. AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity. IJRSM. 2019;6(3):50-61.
40. Dalal A. Designing Zero Trust Security Models. SSRN. 2021:5268092. Preprint. doi:10.2139/ssrn.5268092
41. Pimpale S. Electric Axle Testing and Validation. 2022.
42. Mishra A. Agile Coaching: Effectiveness and Best Practices. 2020.
43. Mohammad A, *et al*. The Influence of Hot Point on MTU CB Condition. J Renew Energy Electr Comput Eng. 2023;3(2):37-43.
44. Hegde P, Varughese RJ. Predictive Maintenance in Telecom. J Mech Civ Ind Eng. 2022;3(3):102-18.
45. Dalal A. LEVERAGING CLOUD COMPUTING TO ACCELERATE DIGITAL TRANSFORMATION. SSRN. 2018:5268112. Preprint. doi:10.2139/ssrn.5268112
46. Pimpale S. Impact of Fast Charging Infrastructure on Power Electronics Design. IJRSM. 2021;8(10):62-75.
47. 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.
48. Mishra A. Analysis of Cyberattacks in US Healthcare. 2022.
49. Mohammad A, *et al*. Design and Implementation of Low Cost MPPT Solar Charge Controller. 2022.
50. Hegde P. AI-Driven Data Analytics: Insights for Telecom Growth. 2020.
51. Dalal A. Maximizing Business Value through AI and ML in SAP Platforms. SSRN. 2019:5424315. Preprint. doi:10.2139/ssrn.5424315
52. Pimpale S. Comparative Analysis of Hydrogen Fuel Cell Vehicle Powertrain. 2020.
53. Mohammad A, Mahjabeen F. Revolutionizing solar energy with AI-driven tech. 2023.
54. Hegde P, Varughese RJ. Elevating customer support experience. 2023.
55. Dalal A. Cybersecurity And Artificial Intelligence: How AI Is Being Used. Turk J Comput Math Educ. 2018;9(3):1704-9.
56. Pimpale S. Optimization of DC Microgrid using non-linear Bang Bang control. 2020.
57. Tiwari A. Generative AI in Digital Content Creation, Curation and Automation. 2023.
58. Mishra A. Leveraging Artificial Intelligence to Improve Cybersecurity Defences. 2020.
59. 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.
60. Mohammad A, *et al*. Revolutionizing solar energy with AI-driven enhancements. 2023.
61. Hegde P. Automated Content Creation in Telecommunications. 2021.
62. Dalal A. Addressing Challenges in Cybersecurity Implementation. SSRN. 2022:5422294. Preprint. doi:10.2139/ssrn.5422294
63. Pimpale S. Efficiency-Driven and Compact DC-DC Converter Designs. 2023.
64. Halimuzzaman M, Gazi MAI, Rahman MS. Journal of Socio-Economic Research and Development-Bangladesh. 2013;10(5):1557-64.