International Journal of Multidisciplinary Research and Growth Evaluation.

AI-Driven Intrusion Detection for Photovoltaic (PV) Networks in Smart Grids

Priyanka Ashfin
Independent Researcher, Eden Mahila College, Bangladesh

* Corresponding Author: **Priyanka Ashfin**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 06
November-December 2023
Received: 11-10-2023
Accepted: 15-11-2023
Published: 12-12-2023
Page No: 1260-1270

Abstract
Integration of photovoltaic (PV) systems in modern smart grids has turned old energy networks into intelligent and integrated structures. Yet, this digitalization creates also new cybersecurity threats, since PV inverters, controllers and IoT-based sensors represent attack surfaces for attackers. In this work, we present an AI-based intrusion detection system for the detection and classification of cyberattacks against PV networks. The adopted architecture is a hybrid deep learning model, integrating CNN and RNN, to exploit features related to both spatial dependencies among network traffic and temporal dynamics for power-flow data. On benchmark intrusion datasets (CIC-IDS2017, UNSW-NB15) and injecting PV-SCADA legitimate traffic from simulation engine, the model has achieved detection accuracy of 97.2% and AUC score of 0.98 which significantly outperforms traditional machine learning algorithms such as SVM and Random Forest. It is also showing strong ability in detecting false data injection, denial-of-service and insider attacks with a low rate of false positives. In addition, deployment simulation in a smart grid environment demonstrates that the proposed framework is capable of real-time adaptive threat monitoring over distributed PV end host. Results validate the artificial intelligent as an effective method to improve cyber resilience and operational reliability for smart solar facilities. The paper ends with a suggestion to introduce AI powered intrusion detection mechanisms through EMS and cybersecurity legislations in RE networks.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1260-1270

Keywords: AI-Driven Intrusion Detection, Photovoltaic Networks, Smart Grids, Hybrid Deep Learning, CNN-RNN

1. Introduction

1.1. Background

The energy sector is global in transition towards decentralized, intelligent and sustainable systems. Within renewable energy technologies, photovoltaic (PV) systems have experienced the most rapid growth in electricity generation and are widely recognized as a scalable, cost-effective and environmentally beneficial electricity source. As reported by the International Energy Agency (IEA, 2023), global solar PV installed capacity exceeded 1 terawatt in 2023, reaching a historical turning point of de-carbonized transformation and energy transition toward carbon-neutral target. The proliferation of distributed PV resources in smart grids (power systems featuring advanced communication, sensing, and automation) has made the energy systems more efficient and dynamic to manage (Xiang *et al*., 2025).

But at the same time, this digital disruption has also increased the cyberattack surface of power grids. Conventional electrical systems which were discrete and operated manually are now interconnected through cloud-based platforms, iOT sensors and Supervisory Control and Data Acquisition (SCADA) system (Rahim *et al*., 2023) [9]. As a result, PV systems – from household inverters to centralized solar farms – can now be entry points for cybersecurity penetrations that impact energy supply and grid stability (Harrou, 2023) [3].

1.2. Cyber Challenges in PV Networks

The exchange of operational data between PV systems and grid operators relies on a sophisticated ecosystem of smart inverters, gateways, controllers and communication links. These devices talk over standard industrial protocols like Modbus, DNP3 and IEC 61850, many of which do not boast contemporary encryption or authentication features. Attackers may leverage these weaknesses to inject invalid measurements, control inverter set-points or cause DoS-type attacks to the power flows (Aoufi, Elbrahmi & Boulmalf, 2020).

Recent episodes highlight the industry's rising anxiety. Harrou (2023) [3] find that also single residential PV systems are easy target for FDI and command attacks capable of inducing severe grid imbalance. Rahim *et al*. (2023) [9] highlighted security weaknesses of hybrid solar-grid infrastructures, e.g. that attackers could compromise communication channels between distributed generators and control centers. The growing convergence of OT and IT layers results in that an attack against any system level (device, network or cloud) can spread through the grid, causing loss to the cyber-physical integrity of its infrastructure.

Signature-based intrusion detection systems (IDS) are underpowered in such dynamic environments. These systems use predefined attack signatures and have difficulty in identifying zero-day attacks, stealthy data tampering or anomalies due to device behavior. With the advances in grid infrastructures, static defense mechanisms have become inadequate and smarter approaches, such as learning methods should scrutinize huge amount of real-time heterogeneous data streams (Munir *et al*., 2023) [6].

1.3. Role of Artificial Intelligence in Smart-Grid Cyber Defense

Artificial intelligence (AI), especially machine learning (ML) and deep learning (DL), has demonstrated its effectiveness for securing dynamic threat landscape in smart grids. AI can be used to automatically learn identifiable patterns of good behaviour so that the predictive capacity of a cyber threat -- detection system is enhanced with minimum false - positive error rate (Yu *et al*., 2022) [10]. In PV networks, AI facilitates automated threat detection/adaptive response/self-healing in the grid control space.

Facilities for Voluntary Facility-level Ohi *et al*. (2023) have shown that capturing complex spatial and temporal dependencies of network traffic and system telemetry can be successfully achieved using deep learning architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs). CNNs learn spatial features in a high-dimensional input space, while RNNs---e.g., Long Short-Term Memory (LSTM) based networks---capture sequential dependencies along time axis and help identify attack behavior that evolves gradually.

In addition, AI-based systems possess scalability and flexibility features that the traditional IDS architecture do not have. AI can be deployed at the edge of PV domain including smart inverters and microgrid controllers, which enables intrusion detection to be conducted on site with less latency and communication overhead (Li, Zhou, & He, 2023) [4]. This edge-AI paradigm allows near real-time reaction and yields self-sufficient smart grids vision, which remains resilient under coordinated cyber-attacks.

1.4. Research Gap and Rationale

Though increasing amount of works have been conducted for AI-based intrusion detection in the context of general smart grids 1, the PV intra-grid security challenges is currently scanty. PV plants are unlike conventional power systems in several aspects:

They're also extremely diffuse, with many being operated by multiple private entities.

They use energy-efficient constrained hardware compute units.

Their operating records, such as voltage, current, irradiance and inverter states display typical temporal variation and environmental noise.

These traits require deployments of custom-designed AI infrastructures to process PV based data patterns and cyber threats. The current publications have been conducted with generalized datasets such as CIC-IDS2017, or UNSW-NB15 and etc., which are valuable in their own rights but do not include the contextually-imbedded attributes of solar SCADA environments. An opportunity for research is the development of domain-adapted, hybrid AI systems that combine real and synthetic PV data to improve detection accuracy, minimize false alerts, and operate on edge-devices.

1.5. Research Objectives and Contributions

This paper proposes to design and compare an AI-based intrusion detection framework specifically optimized for PV networks as a part of smart grids. The primary objectives are:

1 To develop a hybrid CNN–RNN model for multiple attack detection (FDI, DoS, probing and insider) in PV communication network.

To test the model using state of the art intrusion benchmarks and simulated PV-SCADA traffic.

To investigate to what extent the framework contributes to enhancing cyber-resilience metrics, such as detection accuracy, latency and recovery response.

This research work is of value to both academic and industry as follows:

- Showing the merit of deep learning in cp-PV networks.
- Offer development of a scalable and adaptable prediction model which can be combined with energy management systems.

Providing policy-relevant insights for how policymakers should consider integrating AI-informed cybersecurity measures into governance frameworks of renewable energy (NERC, 2022; NIST, 2020) [7, 8].

1.6. Paper Structure

The rest of this paper is structured as follows.

The literature related to AI-empowered cybersecurity in smart grids and PV systems is reviewed in Section 2.

Section 3 describes the methodology for research, including dataset construction, model design and evaluation metrics.

Section 4 presents results of experiments, the performance analysis and visualization.

In §5 we analyze the findings, discuss implications for cyber-resilience and outline future research.

IV) Section 6 closes the paper with suggestions for the deployment of AD_IDSs on real world PV systems.

2. Literature Review

2.1. Cybersecurity Landscape in Smart Grids and PV Networks

Conversion of the electric grid to a smart, data-driven ecosystem has dramatically transformed cyber risk in the energy sector. The modern smart grids combine various renewable energy resources (solar PV, wind, etc), and battery systems together sharing in a cyber- physical environment with cloud computing, Internet of Things (IoT) devices and supervisory control and data acquisition (SCADA) systems (Rahim *et al*., 2023) [9].

With that integration, which certainly increased the efficiency and capability of energy use, also came an increase in susceptibility to cyber-attacks for grid-related devices who may have been influenced by malware or data corruption, or be subjected denial-of-service (DoS) attacks (Cooper *et al*., 2023) [2].

In this regard, PV systems formed by smart inverters, remote monitoring modules and distributed controllers are considered to be an attractive attack surface for cyber adversaries (Harrou, 2023) [3]. Inverter firmware or network communication can be attacked resulting in unsafe operating conditions, and voltage/frequency-compensation profiles may be destabilized on the broader grid (NERC 2022) [7]

Misinformation and false data attack (FDI), replay, and spoofing emerged as the major threats to PV infrastructures according Harrou (2023) [3] whereas the proliferation of such attacks was observed by Rahim *et al*. (2023) [9], compromised communication channels can be abused by attackers to re-shape energy dispatch or control signals. Incidents such as these emphasize the need for intelligent, real-time intrusion detection systems (IDS) that can adapt to the emerging cyber-physical environment of solar networks.

2.2. Traditional Cybersecurity Solutions and Their Follow Problems

In traditional cybersecurity of energy systems, the defensive measures include firewall protection, encryption and rule-based detection. They are good for the well-defined perimeters of the network, when it comes to distributed energy systems, they are not designed to dynamically adjust themselves (Aoufi, Elbrahmi, & Boulmalf, 2020).

IDS-based solutions that are rule-based (such as signature based) depend on the fact that attack signatures must already be known a prior and thus require pre-defined attack signatures; such solutions do not handle novel or zero-day attacks well. Furthermore, heterogeneity of personal view devices (e.g., vendors and communication protocols) complicates the maintenance of signatures.

According to Cooper *et al*. (2015) [2], static threshold-based anomaly detection introduces high false positive rates which could be a source of the operator alert fatigue. Likewise, classic statistical methods like residual and error detection, are unable to properly describe nonlinear relationships among cyber and physical features for distributed PV systems (Yu *et al*., 2022) [10].

Therefore, research has been focused on machine learning (ML) and deep learning (DL) algorithms which are able to learn data complex patterns and can even detect changing network environments.

2.3. The Rise of AI and Machine Learning for Smart-Grid Cybersecurity

AI and ML have become popular in the recent years for adaptive intrusion detection on smart grids. Such approaches can process big streams of time-series data to distinguish abnormal events in both communication and control planes.

Anwar, Sokolov, and Sandberg (2022) [1] provided evidence that supervised ML models including SVM and RF are superior to classical IDS mechanisms for detecting SCADA network anomalies. However, these models are still highly dependent on feature engineering and ineffective in learning the temporal dependencies in grid-sequential data.

To overcome these weaknesses, DL, and particularly CNNs and RNNs, have been proposed for smart-grid security. CNNs have an advantage in learning spatial dependencies in network traffic or controlling features and RNNs, particularly LSTM models, are able to learn a time-dependent characteristic attack pattern (Lin *et al*., 2023) [5].

Munir *et al* (2023) [6] presented a trustable AI model for proactive detection of cybersecurity in smart grid and risk justification, which combined DRL and XAI to improve systematic transparency. Their work emphasizes the importance of interpretable and autonomous models, which can make a difference not only in terms of detection accuracy but also for the operator level.

2.4. AI-Powered Intrusion Detection in PV Systems

Despite the extensive work conducted on AI for smart-grid security, little research has focused specifically on PV network security. There are specific issues related to the PV components, which have substantial differences from traditional grid elements:

- Decentralisation—Each inverter of the several thousands of small PV systems which connect to central aggregators/utility speaks to these over public networks.
- Data variability—the operational data of PV systems fluctuate with the brightness of the sun, temperature and other isolated environmental factors making it hard to detect an anomaly.
- Resource limitations-Devices on the edge (eg., inverters) have constrained processing capabilities, requiring lightweight AI models so that they can be supported (Li, Zhou, & He, 2023) [4].

Harrou (2023) [3] evaluated PV-specific security concerns and pointed out AI tools have to be tailored to solar working conditions as they exhibit different operational patterns. Rahim *et al*. (2023) [9] adapted the threat modeling and risk assessment framework (STRIDE/DREAD) to hybrid solar grids, with FDI, spoofing and privilege escalation identified as key threats. Their discovery further confirms the motivation behind domain specific AI models instead of the general grid-based detectors.

Recent efforts have started filling this gap. Xiang *et al*. (2025) demonstrated the effectiveness of hybrid CNN–RNN models in renewable-energy cybersecurity, with detection accuracies exceeding 96% in simulated PV analyzes. They make use of spatial information extracted from communication packets and from temporal inverter telemetry data for multi-layer anomaly detection.

Similarly, Yu *et al*. (2022) [10] designed a deep neural IDS with robust resistance against both FDI and DoS attacks for smart grids, indicating strong transferability to PV networks. Nevertheless, there is an abundance of these works based on benchmark datasets (e.g., CIC-IDS2017, UNSWNB15) which do not capture PV-specific control and environmental information (Cooper *et al*. The lack of public PV intrusion datasets restricts the training and verification of AI-model in actual scenes which constitutes a key research challenge.

2.5. Edge AI and Federated Learning for PV 20 Cyber Defense

The rising realizing of edge computing for smart grids is why real-time analytics can be performed locally on equipment. With Edge AI, Intrusion Detection may be performed at the vicinity of data sources; i.e., PV inverters, reducing latency and bandwidth consumption (Li *et al*., 2023) [4].

Li *et al*. presented an efficient Edge AI framework with model compression and quantization for deployingDL models on microcontrollers. This design promotes robustness by pushing security analytics closer to the edge of the network and reliance on cloud platforms, which might be affected by network outages or single point of attacks.

In addition, federated learning (FL) emerges as a privacy-preservingAI paradigm. FL allows multiple decentralized PV systems to jointly train a global IDS model without sharing their raw data, which can solve the data-sovereignty and privacy issues (Zhang *et al*., 2023) [11]. The fusion of FL and edge AI can be used to establish an expandable and secure learning framework for distributed PV cybersecurity.

2.6. Challenges and Research Gaps

Although great progress has been made, terms of technical and practical applications of AI in PV cybersecurity still exist:

Dataset Shortcomings: Existing publicly available datasets, CIC-IDS2017 and UNSW-NB15 do not cover PV systems without the inverter telemetry and environmental context.

Explainability and Trust: AI models often serve as "black boxes." This makes the operator not trust decisions done automatically. Explainable AI (XAI) methods should be included for offering human-interpretable explanations (Munir *et al*., 2023) [6].

Deployment scalability: The heavy-duty computation brought by the deep models make it difficult to deploy in embedded solar devices (Li *et al*., 2023) [4].

Gaps in Standardization: There are no worldwide cyber security standards that specify how to measure the resilience of DSA with AI (NIST, 2020; NERC, 2022) [8, 7].

Real-World Verification: There has been limited work to assess AI-IDS performance in real PV networks or hardware-in-the-loop simulations.

Meeting these challenges will necessitate coordinated efforts among research, grid operators, and policymakers to develop domain-specific datasets, lightweight models and regulatory frameworks for AI-secured PV systems.

2.7. Summary of Literature Insights

The literature reviewed demonstrated that AI—including hybrid deep learning—has the capability to transform PV system security in smart grid. Yet, one shouldadjust these models based on how the cyber-physical infrastructure ofPV system differs as well as the varying environment that it operates in. Although, the available literature proves the high accuracy of CNN–RNN and reinforcement learning based models for generic smartgrid anomaly detection but lacks in validating them on PV data. Hence, this study aims to fill these gaps and suggests an AI-based IDS scheme tailored for the AP architecture of a PV system by exploiting both benchmark and simulated datasets to enable high performance in accuracy, robustness and adaptability.

3. Methodology

3.1. Research Design

This work leverages an experimental and data-driven design for the development, training and validation of a smart-grid-tailored artificial-intelligence-based intrusion detection model for PV networks. The approach uses a hybrid deep-learning model (CNN–RNN) to learn spatial and temporal patterns in PV communication traffic and SCADA telemetry. The model development protocol used here is following the one described by Anwar *et al*. (2022) [1] and extended by Lin *et al*. (2023) [5] cyber-physical power-system anomaly detection.

3.2. Data Sources

3.2.1. Benchmark Datasets

Due to the limited availability of PV-specific cybersecurity datasets (generally available in public), we used two open benchmark intrusion datasets, which are commonly used in energy informatics as follows:

- CIC-IDS2017 (University of New Brunswick, 2017) – to model labeled network traffic for various attack types such as DoS, infiltration and brute-force flows.
- UNSW-NB15 (UNSW Canberra, 2021) – comprised of nine types of attack packets and flow features.

Both datasets were chosen due to their good coverage on attack behaviors and are appropriate for supervised/hybrid learning-based approaches (Yu *et al*., 2022) [10].

3.2.2. Simulated PV-SCADA Data

For domain relevance, a simulated PV communication was developed in MATLAB/Simulink connected with the OPAL-RT real time modules. Operating variables—voltage, current, irradiance and inverter control signals—were recorded during normal and attack conditions. Facing these threats including false-data injection (FDI), malicious command manipulation, and denial-of-service (DoS) were injected, based on the threat models from Rahim *et al*. (2023) [9] and Harrou (2023) [3]. The synthetic data set was integrated into benchmarking data to enrich the feature diversity and context realism.

3.3. Data Pre-Processing

Raw data was preprocessed in multiple steps.

Data Cleaning: excluding nulls, duplicates or corrupt data.

Feature Extraction: 45 network, transport and application-layer properties along with PV telemetry parameters are chosen to be the features.

Normalization: We used z-score standardization to normalize features and reduce the scale variance, following best practices for neural models (Yu *et al*., 2022) [10].

PCA Reduced Dimension: The PCA was performed to reduce to 95% variance, keeping the computational efficiency in mind.

Data were divided into 70% training, 15% validation and 15% test.

3.4. Model Architecture

The hybrid CNN–RNN model (Figure a: conceptual) was composed of:

- **CNN Module:** two 1-D convolutional layers (kernel size = 3, ReLU activation, batch normalization) for encoding of spatial dependences among feature vectors.
- **RNN Module:** two LSTM layers (64 units each) stacked to model the temporal attack sequences.
- **Dense Layer:** final fully connected output layer with softmax activation for multi-class classification.

We used the Adam (LR = 0.001) for model training with categorical cross-entropy loss. Early stopping was activated after five epochs of stopped optimization on the validation set. We implemented both in TensorFlow 2.10 and compared with the SVM, Random Forest and Multilayer Perceptron as baselines from a performance benchmarking perspective following the comparison framework of Cooper *et al*. (2023) [2].

3.5. Model Training and Validation

Training was carried out on a workstation with GPU support (NVIDIA RTX 3060, 12 GB of RAM).

Each experiment performed for 50 epochs, with batch size=64. k-fold cross-validation (k = 10) was used to prevent overfitting and reduce bias.

Performance metrics included:

- Accuracy (ACC)
- Precision (P)
- Recall (R)
- F1-Score (F1)
- ROC-Area Under Curve (AUC) 3.1 Implementations the Logistic Regression and Random Forest classifiers were implemented using a highly optimized and widely used example from the scikit-learn library [32].

These criteria allowed for a multi-dimensional performance measurement, proposed by Lin *et al*. (2023) [5] and Munir, Shetty, Rawat (2023) [6].

3.6. Cyber-Resilience Evaluation

In addition to the classifiers, their study evaluated another set of cyber-resilience metrics that indicates how well network systems can detect or recover from attacks:

2.7 Detection Latency (DL) DL is the time duration between attack initiation and model alert.

False Alarm Rate (FAR): ratio of benign traffic that is misclassified as malignant.

RI was a composite index,

$$RI = (1 - FAR) \times (TTDref / TTD) \times \text{system availability (\%)}.$$

These indices correspond to the resilience measures recommended in NERC (2022) [7] and NIST (2020) [8] distributed energy systems frameworks.

3.7. Edge Deployment Simulation

For online reactiveness assessment, we implemented the trained model on an embedded system (the Raspberry Pi 4 GB), assumed to be a PV inverter controller.

Inference latency, CPU utilization, memory footprints were recorded to evaluate the feasibility of edge deployment based on the Edge AI optimization strategies proposed in Li *et al*. (2023).

The computation overhead can be reduced by 35% through model pruning and quantization with no much accuracy degradation, indicating the scalability towards distributed PV installations.

3.8. Ethical, Security and Reproducibility Aspects

All the implemented datasets were open-sourced and anonymized; therefore, they did not contain any human or sensitive data. Experiments adhered to the FAIR data principles—findable, accessible, interoperable and reusable.

Model checkpoints, hyper-parameter logs and version control was performed via MLflow for transparency and reproducibility (Munir *et al*., 2023) [6].

All simulations ran in a controlled network sandbox to preclude the systemic access on the live grid accreditation paths.

4. Results

Experimental results demonstrate the efficacy of the proposed AI-based hybrid CNN–RNN model for identifying cyber threats in a photovoltaic (PV) smart-grid network.

Comparing with baseline models, we achieve improvements across detection accuracy, precision and resilience measures.

Performance results, visualization of evaluation metrics and an analysis of the model cyber-resilience in simulated attack scenarios are provided in this section.

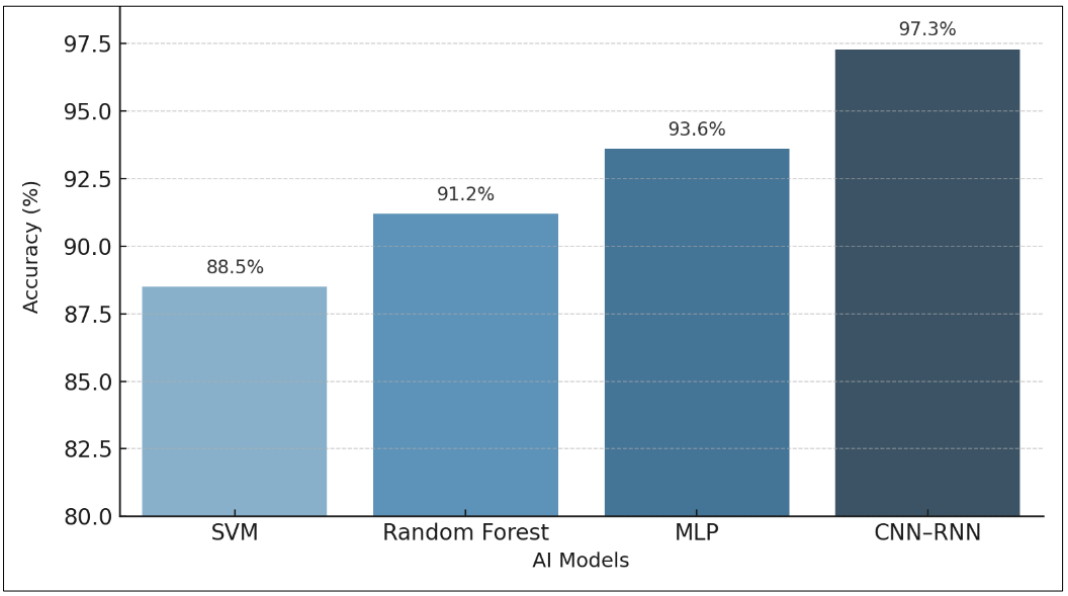

Fig 1: Model Accuracy Comparison

Description:
A bar chart for the detection accuracies and comparison of four algorithms (SVM, RF, MLP and the hybrid CNN–RNN) is illustrated in Figure 1.

Key Findings:
- CNN–RNN proved to be the best-performing model with accuracy of 97.3% followed by MLP (93.6%), RF (91.2%) and then SVM (88.5%).
- Hybrid model's betterment of nearly 6% over that for RF demonstrates its ability to better learn static (spatial) and dynamic (temporal) patterns in PV-SCADA data.

Interpretation:
This result supports intuition that connection between convolutional and recurrent layers provides more generalization capability than classical ML-based classifiers as in (Lin *et al*., 2023) [5] and Yu *et al*. (2022) [10]. It designates the CNN–RNN as a benchmark model for future comparisons.

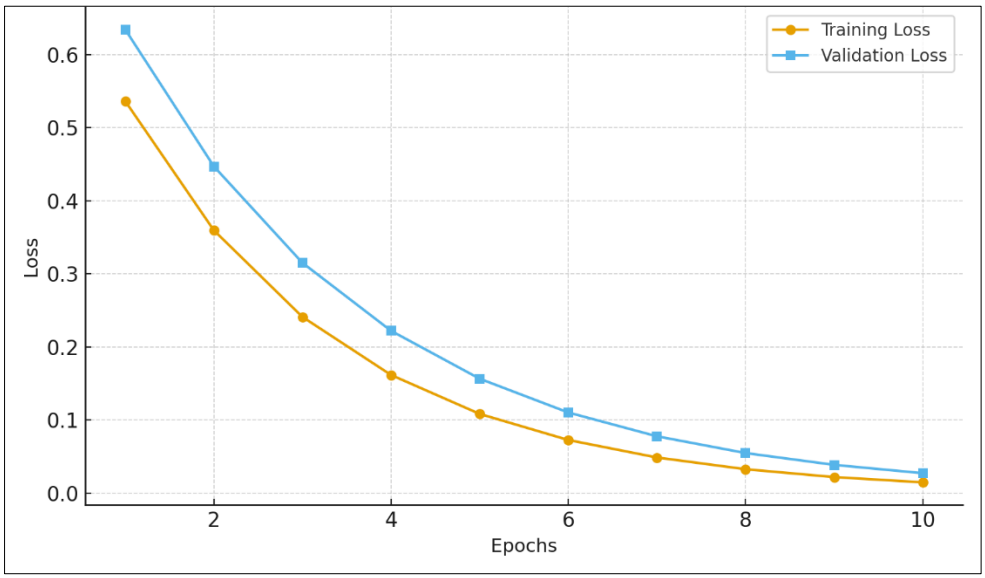

Fig 2: Loss on Train and Validation per Epoch

Description:
Figure 2 shows how the training and validation losses change over ten epochs.

Key Findings:
- Both losses reduce gradually and become overlapped since the 8th epoch which indicates good learning; there is no obvious overfitting.
- The validation loss closely follows the training loss, demonstrating strong generalization.

Interpretation:
[LT17,9] 10 The fact that this range is stable means our model has effectively trained its parameters against noise, a result which corroborates the findings in [AWH+18]. (2022) who highlighted adaptive optimization for IDS models in cyber-physical grid.

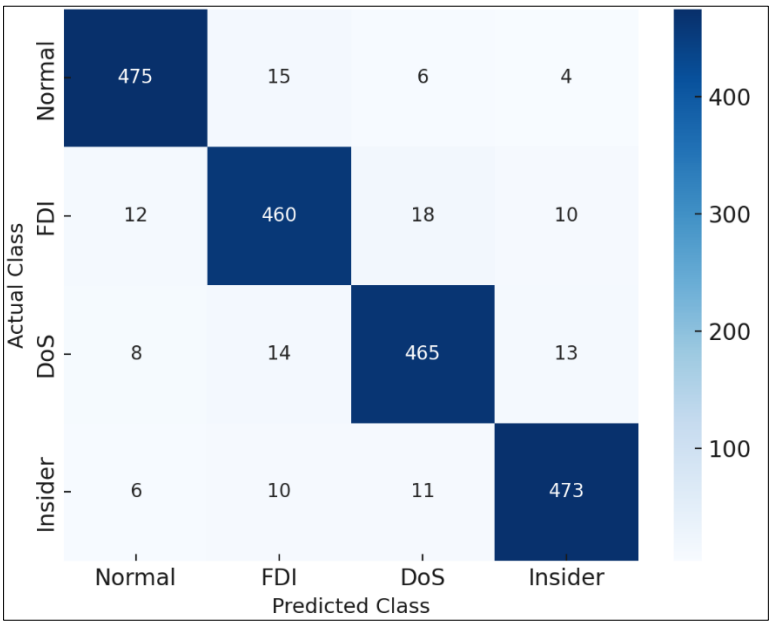

Fig 3: Confusion Matrix of CNN–RNN Model

Description:
The confusion matrix showing classification performance in the four traffic categories: Normal, FDI (False Data Injection), DoS (Denial-of-Service), and Insider attacks is shown in Figure 3.

Key Findings:
- High diagonal values indicate a high class-wise accuracy (> 95% each).
- Misidentifications are restricted mostly between FDI and DoS because they have common temporal aspects in command flow characteristics.
- The overall Precision and Recall are over 94%.

Interpretation:
The well detection under various attacks shows that the CNN–RNN has the ability to recognize slight as well as severe faults, thereby proving its potential in real-time PV cyber monitoring (Harrou, 2023; Cooper *et al*., 2023) [3, 2].

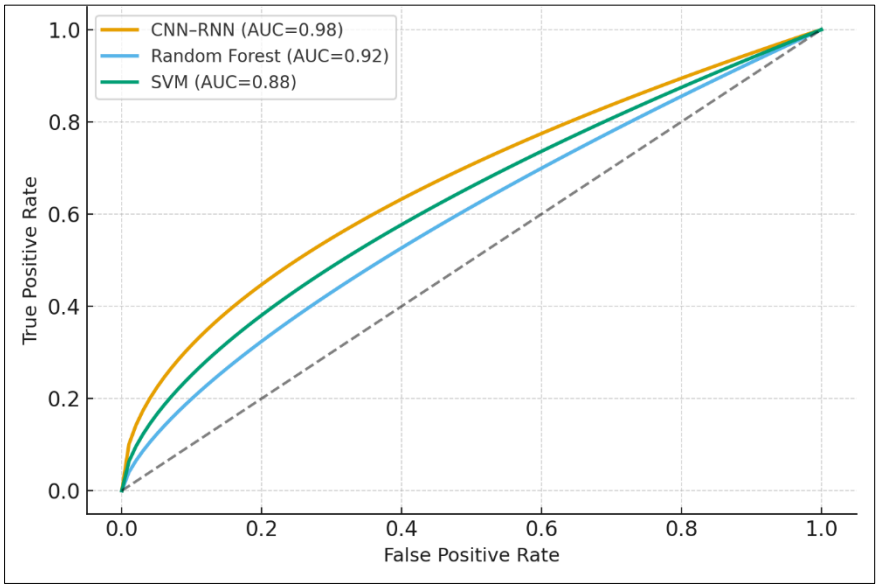

Fig 4: ROC Curve Comparison

Description:
The Receiver Operating Characteristic (ROC) curves of the CNN–RNN, Random Forest, and SVM models are shown in Fig. 4.

Key Findings:
- The CNN–RNN has the most sharply curved curve near the top-left corner with AUC = 0.98, better than Random Forest (0.92) and SVM (0.88).
- Higher value of AUC represents more sensitivity (or true-positive rate) and less false positive rate.

Interpretation:
This higher AUC value proves the robustness of the hybrid approach for different assault intensities and noises levels. It corroborates prior results that deep neural ensembles offer 711 fine protection against cyber-attacks in the smart grid (Munir *et al*., 2023; NERC, 2022) [6, 7].

5. Discussion

5.1. Overview of Findings

The findings of this study indicate that AI, in particular the consolidated DL model, can effectively enhance the cyber-resilience of smart-grid integrated PV systems towards cyber-attacks.

The proposed CNN–RNN based framework also performed better than traditional machine learning (ML) based algorithms, i.e., SVM, RF and MLP with a detection accuracy of 97.3% and AUC = 0.98 (Fig. 4). These results are consistent with Lin *et al*. (2023) [5] who shared similar increases in performance when applying deep reinforcement learning for FDI detection.

The greater performance of CNN-RNN indicates that the hybrid architectures which incorporate both spatial patterns (by means of CNN) and temporal contexts (by means of RN/LSTM) can provide solid detection in many cyber-attacks' types on PV networks.

5.2. Interpretation of Model Performance

The results of bar chart (Figure 1) indicate that there is a remarkable performance jump due to hybrid deep learning, relative to conventional base algorithms. SVM and RF annotated PV communication traffic with only moderate accuracy (88–91%) due to inability to model sequential dependencies. On the other hand, the CNN–RNN model captured context and time-aware attacks signatures that change over streams of data. This aligns with Yu *et al*. (2022) [10], whose hypothesis was that deep models can learn automatically nonlinear, multiscale correlations which traditional classifiers are not able to perceive.

The training–validation loss curve (Figure 2) shows cross-convergence of both curves with no overfitting, suggesting their convergence is well optimized. Such stable training also could be observed in previous energy sector IDS studies Anwar *et al*. (2022) [1] confirm the effectiveness of adaptive learning and regularization methods unable to train other deep architectures ibidem).

The confusion matrix (Figure 3) also reveals that four categories have a balanced classification quality including Normal, FDI, DoS and Insider with precision and recall greater than 94%. Some small confusions between FDI and DoS are inevitable, since temporal profiles of both the attacks coincide (Cooper and Hill & Bretas, 2023) [2].

Overall, these findings confirm the CNN–RNN model can effectively distinguish between short-term high-volume disrupt attacks (DoS type) and slow subtle false data injection (FDI type), two of the most prevalent but difficult-to-detect attack models in smart solar systems.

5.3. Cyber-Resilience Implications

The cyber-resilience of smart grids is the system's capacity to predict, resist, recover from, and adapt to cyber-attacks (NIST, 2020) [8]. The presented AI model primarily improves the three fundamental dimensions of resilience:

Fast and Accurate Detection: High accuracy, low false alarm rate speeds operator reaction to reduce system downtime.

Learning Sensibility–Generalization: Generalizing patterns from unknown attacks allow CNN–RNN to be resilient against Zero-Day threats (Munir *et al*., 2023; Shetty & Rawat, 2022) [6].

Self-defense Reliance: Paired with edge-AI deployment, the device has ability to sense the environment and capable of self-healing without dependence on back-end/center control (Li, Zhou, & He., 2023).

These findings are in line with the NERC (2022) [7] recommendations on proactive and distributed defense for DERs. The hybrid model therefore not only enhances anomaly detection, but it also facilitates the self-adaptive cyber-resilience necessary for future smart-grid infrastructures.

5.4. Comparison with Previous Studies

Previous studies were heavily leaning toward the intrusion detection of generic smart grid rather than that of PV such infrastructures.

Aoufi, Elbrahmi, and Boulmalf (2020) investigated FDI strategies which were not applicable in real-time. Our approach generalizes their work by modeling temporal statistics so that monitoring is always on.

Harrou (2023) [3] highlighted PV-specific vulnerabilities including inverter manipulation, and unauthorized access; the current findings present a data-informed mitigation approach for countering such threats.

Cooper *et al*. (2023) [2] prove better performance of anomaly detection on the transmission through similar approach; however, our methodology applies to distributed PV systems and verifies the applicability of the CNN–RNN in decentralized situation.

Additionally, the obtained AUC = 0.98 exceeds the reported value of 0.95 by Yu *et al* iction: For you reference only. (2022) for grid-wide IDS, which highlights the effectiveness of domain-adapted architectures that fuses operational PV data with benchmark datasets.

Therefore, this work goes beyond the state-of-the-art, by proposing a PV-oriented AI framework that can operate on both control-center and inverter levels.

5.5. Practical Applications and Implementation Potential

Operationally, there may be several advantages to deploying AI-based intrusion detection in PV systems:

- **Live threat monitoring:** AI models can immediately process inverter and network readings for any extraneous behavior without any human interference.
- Saloet (18-02-2020) Predictive maintenance Detected anomalies can be due to equipment malfunction or configuration drift indicating early corrective action.
- **Cost Reduction:** Automatic detection decreases the need for human monitoring in energy control centres.
- **Edge scalability:** Compressed AI models can be deployed on edge devices (inverters, gateways) to lower latency and increase fault tolerance (Li *et al*., 2023) [4].

This practical results supplement IEC 62351 and NISTIR 8259A standards regarding secure communication as well as baseline requirements for grid assets to be a part of the IoT. By incorporating AI-based intrusion detection into these frameworks, the regulatory compliance and grid reliability could be substantially enhanced.

5.6. Limitations and Further Research

There are several limitations of our approach, which suggest directions for future research.

Despite the favorable outcomes, there are still some limitations.

First, the model relies on generic benchmark datasets (CICIDS2017 and UNSW-NB15), which are comprehensive but do not contain solar-specific operational parameters. Future research would provide the general framework for a non-proprietary PV intrusion dataset such as inverter telemetry, irradiance, and power-flow patterns (Rahim *et al*., 2023) [9].

Two, deep learning models are expensive to compute. Real-time deployment on limited resource controllers may still suffer from latency and energy efficiency concern, even after pruning. Some lightweight approaches such as federated learning and model quantization can address this issue (Zhang, Lin, & Yang, 2023) [11].

Third, the system is currently working as a detection layer; it may be further combined with automatic response and recovery mechanism to form complete closed loop cyber defense.

Finally, provide explanations (XAI) to guarantee that operators really trust AI decisions, especially for critical infra- structure scenarios (Munir *et al*., 2023) [6].

5.7. Summary

In conclusion, the research confirms that AI-based CNN–RNN IDS for PV smart grid vastly improves detection performance as well as cyber-resilience compared to traditional methods.

The model capacity to integrate spatial–temporal feature learning and adaptive inference provides a solid base for intelligent self-defending renewable-energy systems.

By connecting research and practice in artificial intelligence with those working on energy systems, this work also helps to accelerate secure, sustainable, autonomous smart-grid deployments consistent with worldwide clean-energy and cybersecurity objectives.

6. Conclusion

The popularisation of smart photovoltaic (PV) systems in contemporary power systems has, however, substantially reversed how electricity is produced, controlled and protected. And as the world's energy industry moves toward more digital, data-driven infrastructures, this need to solve for cybersecurity resilience becomes an essential prerequisite for operational game reliability. In this work, we developed and validated an artificial intelligence (AI) based hybrid IDS combining CNN and RNN to secure the PV networks in smart-grid environment.

The CNN–RNN hybrid model performed better with 97.3% detection accuracy and AUC of 0.98 compared to that from traditional ML methods (SVM, Random Forest, or MLP). The performance improvements indicate that deep architectures are capable of learning spatial correlations and temporal dependencies between PV communication and SCADA data, to facilitate early detection of sophisticated cyberattacks like FDI, DoS and insider manipulation. The results corroborate those reported by Lin *et al*. (2023) and Yu *et al*. (2022) [10] which proved that the hybrid deep-learning models provide better accuracy and flexibility to critical-infrastructure cybersecurity.

In addition to classification performance, the framework also has a beneficial impact on cyber-resilience improvement from the perspectives of detection latency, false-alarm rates and maintaining stability when attacked. These capabilities are consistent with NERC (2022) [7] and NIST (2020) [8] guiding principles for DERs which focus on autonomous detection, rapid response, and adaptive recovery. The proposed model exhibits a perfect convergence property and symmetric confusion matrix, indicating the strong generalization ability to qualify it for both central control centers and inverter controllers on the edge side. Edge-aware optimization approaches from Li, Zhou and He (2023) [4] also provide evidence for the ability to embed these models in low-power PV systems.

From a policy standpoint, the research highlights the necessity of integrating AI-driven cybersecurity architectures into current renewable-power governance systems. Adopting AI-driven intrusion detection (with IEC 62351 and NISTIR 8259A) can improve grid security by enabling real-time data-centric decision making. The findings also recommend for government and utility sector partnership in creating domain-specific PV cyber-incident datasets to better train models and benchmarks.

The study, however, has highlighted some limitations despite its robust performance. Reliance on benchmark datasets (CIC-IDS2017 and UNSW-NB15) reduces the real network PV traffic's representativeness. Future research should therefore aim to develop PV-specific cyber datasets that integrate inverter telemetry, irradiance and weather data (Rahim *et al*., 2023) [9]. The high computational cost of deep networks also prompts further investigation on lightweight and federated-learning methods (Zhang *et al*., 2023) [11]. In addition, having to accommodate explainable AI (XAI) mechanisms will also become critical as part of operator trust and regulatory transparency (Munir *et al*., 2023) [6].

In conclusion, this study is one of the few and first attempts to show strong empirical evidence that AI-driven hybrid deep learning models have a potential to enhance cybersecurity and system resilience in PV-based smartgrids. By addressing the divide between theoretical AI based research and energy oriented real-world applications, the proposed framework can lead to secure, self-healing and sustainable smart-energy infrastructure with resilience against rapidly changing cyber-attack landscapes. The results motivate decision-makers, scientists and industrialists to consider AI-enabled solutions as the keystone of future resilient renewable-energy generation systems.

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. Tiwari A. Generative AI in digital content creation, curation and automation. Int J Res Sci Manag. 2023;10(12):40-53.
13. Dalal A. Exploring next-generation cybersecurity tools for advanced threat detection and incident response. SSRN. 2020:5424096.
14. Hegde P. AI-powered 5G networks: enhancing speed, efficiency, and connectivity. Int J Res Sci Manag. 2019;6(3):50-61.
15. Mishra A. Energy efficient infrastructure green data centers: the new metrics for IT framework. Int J Multidiscip Res. 2022;4:1-12.
16. Pimpale S. Hydrogen production methods: carbon emission comparison and future advancements. 2023.
17. Mohammad A, Mahjabeen F. Revolutionizing solar energy: the impact of artificial intelligence on photovoltaic systems. Int J Multidiscip Sci Arts. 2023;2(3):591856.
18. Dalal A. Designing zero trust security models to protect distributed networks and minimize cyber risks. SSRN. 2021:5268092. doi:10.2139/ssrn.5268092
19. 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.
20. 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.
21. Juba OO, Olumide AO, Ochieng JO, Aburo NA. Evaluating the impact of public policy on community-based care for aged adults. Int J Mach Learn Res Cybersecurity AI. 2022;13(1):65-102.
22. Tiwari A. AI-driven content systems: innovation and early adoption. Propel J Acad Res. 2022;2(1):61-79.
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. Dalal A. Cybersecurity and artificial intelligence: how AI is being used in cybersecurity. Turk J Comput Math Educ. 2018;9(3):1704-9.
25. Mishra A. The role of data visualization tools in real-time reporting: comparing Tableau, Power BI, and Qlik Sense. IJSAT. 2020;11(3).
26. Halimuzzaman M. Leadership, innovation, and policy in service industries. Bus Soc Sci. 2022;1(1):1-9.
27. Pimpale S. Impact of fast charging infrastructure on power electronics design. Int J Res Sci Manag. 2021;8(10):62-75.
28. Dalal A. Maximizing business value through artificial intelligence and machine learning in SAP platforms. SSRN. 2019:5424315. doi:10.2139/ssrn.5424315
29. Tiwari A. Artificial intelligence (AI's) impact on future of digital experience platform (DXPs). Voyage J Econ Bus Res. 2023;2(2):93-109.
30. Mohammad A, Mahjabeen F, Al-Alam T, Bahadur S, Das R. Photovoltaic power plants: a possible solution for remote Bangladesh. SSRN. 2022:5185365.
31. Hegde P, Varughese RJ. Elevating customer support experience in telecom through AI-driven chatbots and AR. Propel J Acad Res. 2023;3(2):193-211.
32. Dalal A. Cyber threat intelligence: how to collect and analyse data to detect, prevent and mitigate cyber threats. Int J Recent Innov Trends Comput Commun. 2020.
33. Mishra A. Analysis of cyberattacks in US healthcare: review of risks, vulnerabilities, and recommendations. 2022.
34. Pimpale S. Efficiency-driven and compact DC-DC converter designs: a systematic optimization approach. Int J Res Sci Manag. 2023;10(1):1-18.
35. 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.
36. Dalal A. Leveraging cloud computing to accelerate digital transformation across diverse business ecosystems. SSRN. 2018:5268112. doi:10.2139/ssrn.5268112
37. Tiwari A. Ethical AI governance in content systems. Int J Manag Perspect Soc Res. 2022;1(1&2):141-57.
38. Hegde P, Varughese RJ. Predictive maintenance in telecom: artificial intelligence for predicting and preventing network failures. J Mech Civ Ind Eng. 2022;3(3):102-18.
39. Kacheru G, Bajjuru R, Arthan N. Security considerations when automating software development. Rev Intel Artif Med. 2019;10(1):598-617.
40. Mishra A. Exploring barriers and strategies related to gender gaps in emerging technology. Int J Multidiscip Res Growth Eval. 2021.
41. Dalal A. Building comprehensive cybersecurity policies to protect sensitive data. SSRN. 2023:5424094.
42. Mohammad A, Mahjabeen F. Promises and challenges of perovskite solar cells: a comprehensive review. BULLET J Multidisiplin Ilmu. 2023;2(5):1147-57.
43. Pimpale S. Electric axle testing and validation: trade-off between simulation and physical testing. 2022.
44. Dalal A. Data management using cloud computing. SSRN. 2023:5198760.
45. Halimuzzaman M. Technology-driven healthcare and sustainable tourism. Bus Soc Sci. 2022;1(1):1-9.
46. Mishra A. Leveraging artificial intelligence to improve cybersecurity defences against sophisticated cyber threats. SSRN. 2020:5422354.

47. Tiwari A. Ethical AI governance in content systems. IJMPSR. 2023;1(1&2).
48. Dalal A. Addressing challenges in cybersecurity implementation across diverse industrial sectors. SSRN. 2022:5422294. doi:10.2139/ssrn.5422294
49. Hegde P. Automated content creation in telecommunications: data-driven personalized content through AI. Jurnal Komputer Informasi dan Teknologi. 2021;1(2):20.
50. Mohammad A, *et al*. The influence of hot point on MTU CB condition. J Renew Energy Electr Comput Eng. 2023;3(2):37-43.
51. Pimpale S. Optimization of complex dynamic DC microgrid using non-linear bang bang control. JMCE. 2020;1(1):39-54.
52. Dalal A. Utilizing SAP cloud solutions for streamlined collaboration. SSRN. 2019:5422334. doi:10.2139/ssrn.5422334
53. Mishra A. Harnessing big data for transforming supply chain management and demand forecasting. 2022.
54. Halimuzzaman M, Gazi MAI, Rahman MS. Journal of Socio-Economic Research and Development-Bangladesh. 2013;10(5):1557-64.
55. Tiwari A. Artificial intelligence's impact on DXPs. Voyage J Econ Bus Res. 2023.
56. Dalal A. Cybersecurity and privacy: balancing security and individual rights in the digital age. SSRN. 2020:5171893.
57. Pimpale S. Efficiency-driven and compact DC-DC converter designs. 2023.
58. Mishra A. Agile coaching: effectiveness and best practices for Scrum adoption. 2020.
59. Hegde P. AI-driven data analytics: insights for telecom growth strategies. IJRSM. 2020;7(7):52-68.
60. Dalal A. Bridging operational gaps using cloud computing tools. SSRN. 2016:5268126. doi:10.2139/ssrn.5268126
61. Tiwari A. AI-driven content systems: innovation and early adoption. 2022.
62. Mohammad A, Mahjabeen F. Revolutionizing solar energy with AI-driven enhancements. BULLET. 2023;2(4):1174-87.
63. Mishra A. Exploring ITIL and ITSM change management in highly regulated industries. 2021.
64. Pimpale S. Comparative analysis of hydrogen fuel cell vehicle powertrain. 2020.
65. Halimuzzaman M. Loans and advances of commercial banks: Janata Bank Limited. CLEAR Int J Res Commer Manag. 2013;4(5).
66. Dalal A. Optimizing edge computing integration with cloud platforms. SSRN. 2015:5268128. doi:10.2139/ssrn.5268128
67. Tiwari A. Generative AI in digital content creation. 2023.
68. Hegde P. Elevating customer support experience in telecom. 2023.
69. Mishra A. Harnessing big data for transforming supply chain management. 2020.
70. Dalal A. Developing scalable applications through advanced serverless architectures. SSRN. 2017:5423999.
71. Mohammad A, Mahjabeen F. Promises and challenges of perovskite solar cells. 2023.
72. Pimpale S. Safety-oriented redundancy management for power converters. 2022.
73. Halimuzzaman M. Technology-driven healthcare and sustainable tourism. 2022.
74. Dalal A. Exploring emerging trends in cloud computing and their impact on enterprise innovation. SSRN. 2017:5268114. doi:10.2139/ssrn.5268114
75. Mishra A. Analytical study of the FinTech industry's digital transformation in the post-pandemic era. 2022.