Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 02| Issue- 12| 2023

Research Article **Received:** 01-11-2023| **Accepted:** 25-11-2023 | **Published:** 10-12-2023

Machine Learning Applications in Cyber Threat Prediction for Solar Microgrids

Ura Ashfin

Independent Researcher Eden Mahila College

Abstract: The incorporation of decentralized solar microgrids in modern electrical grids has promoted energy efficiency and sustainability, but such addition constructs a broad common attack surface in interconnected infrastructures. Traditional Intrusion Detection Systems (IDSs) may find it difficult to accommodate the dynamic and data-rich scenario in smart microgrids; hence, there is demand for predictive and intelligent cybersecurity approaches. One such solution is characterized in this work, which investigates the use of machine learning (ML) for predicting cyber threats in solar microgrids and preventing attacks, including false data injection, denial-of-service and spoofing. A ML hybrid model(integrated with CNN and LSTM networks) was proposed to extract the spatial-temporal feature from sensor data and communication network flow. Test results show that the proposed model can reach 96.8% detection accuracy and it has a lower false alarm rate than rule based method does. The combination of ML-based predictive analytics offers up-to-the-minute situational awareness for proactive threat mitigation and operational resiliency. This study demonstrates the promise of smart data-driven solutions for improving cybersecurity in renewable energy networks and contributes to the efforts towards self-learning defense mechanisms for future solar microgrids.

Keywords: ML, Solar Microgrids, Cyber Threat, CNN.

INTRODUCTION

The Move toward solar microgrids which is a vital aspect of the next-generation smart grid ecosystem has been catalysed by the world's move towards renewables. These de-centralised energy systems combine PV panels with battery storage and smart control units to offer stable, environmentally friendly and independent of a grid access to electricity (IEA, 2023). The digitalization of solar microgrids—which supports sensors, Internet of Things (IoT) devices and Supervisory Control and Data Acquisition (SCADA) systems—has allowed for real-time monitoring and enhanced power control. This hyperconnectivity has, however, opened energy systems to a new range of cybersecurity risks capable of threatening data integrity, operational integrity and grid stability (Anwar, *et al.,* 2022; Umar, *et al.,* 2023).

Cyber-attacks to the energy system have been increasing in frequency and complexity, as a result of adversaries exploiting vulnerabilities on communication protocols, cloud interfaces, and control software (Zhang, *et al.,* 2023). In distributed solar microgrids, devices are naturally diverse and the communication links become heterogeneous, which expands the attack surface, resulting in complexity of intrusion detection and response (Kumar, *et al.,* 2022). For instance, false data injection (FDI), denial-of-service (DoS), spoofing and ransomware attacks may corrupt the sensor readings so as to reject power dispatch commands or conclusively result in misbehavior during inverter synchronization operation (Al Garni *et al.,* 2021). Furthermore, the 2020 hacking incident in a European control room of a renewable energy system where attackers shut down grid dispatch controls on a rare occasion provided shocking demonstration for what harm such vulnerabilities can cause to operations and finance (Solar Power Europe, 2021).

Conventional rule-based intrusion detection systems (IDS) and firewalls may not be effective to detect unknown or evolving cyber threats especially in distributed data-centers. Such systems depend on predefined signatures and are not efficient in zero-day attacks or adaptive attacks (Bansal *et al.,* 2021). To mitigate these challenges, machine learning (ML) has recently been identified as a promising approach to intelligent threat prediction and adaptive defense in CPSs (Liu *et al.,* 2023). The ML based approaches are effective in learning complex non-linear pattern from large-scale datasets and generalizing to detect anomalies which are not seen during normal operation of the system (Sahu, *et al.,* 2022).

Recent developments in deep learning (DL)—a subset of ML—have provided an additional leap to cybersecurity analytics by allowing automatic discovery of higher order representations from network and sensor data. For example, CNN is good at spotting the spatial correlations in infocommunication traffic, and LSTM well captures temporal dependencies in time-series data (Zhang, *et al.,* 2023). The joint CNN-LSTM models have achieved the great success in stealthy cyber intrusions detection in smart grids, being superior to classic ones in terms of accuracy and generalization capability (Hossain, *et al.,* 2023). In solar microgrids, these properties are useful to

***Corresponding Author:** Ura Ashfin

DOI- https://doi.org/10.5281/zenodo.17593529

distinguish between genuine environmental changes (e.g., irradiance variations) and the attacks manipulating the data.

Further, advanced threat intelligence, delivered through predictive analysis and supported by methods such as supervised learning and reinforcement based algorithms has the potential to foresee emerging attacks before they materialize, enabling a paradigm of proactive security rather than that of reactive protection (Sharma & Singh, 2023). Methods, such as Support Vector Machines (SVM), Random Forest (RF) and Deep Q-Learning (DQL), are employed to identify a network traffic pattern in filtering defensive strategies against the real-time network traffic pattern so that the network is protected timely (Kouhdaragh, *et al.,* 2021; Yuan, *et al.,* 2022). Such smart systems are in line with the vision of autonomous cyber security in the energy domain – where self-learning algorithms autonomously respond to new threats without human interference.

In this scenario, we address in the current work machine learning based solutions for cyber threat forecasting for solar microgrids. The first task is the hybrid CNN–LSTM model to be trained for prediction and detection of sophisticated cyberattacks in PV-based microgrid environment. The model accepts multi-dimensional input features from communication, inverter and environment data streams to detect known and unknown intrusions. The model is also compared with usual ML algorithms in accuracy, false positive rate and detection time.

Through the predictive power of ML, this study seeks to improve cyber resilience and operational reliability for solar microgrids. The results add to the developing area of AI-empowered cybersecurity for renewable power systems and express palpable advice regarding how creaturely threat monitoring could be incorporated into practical field deployed distributed power infrastructures.

The rest of this paper is structured as follows: Section 2 surveys the related literature on ML-based approaches for smart grid cybersecurity; Section 3 discusses methodology, and hybrid model architecture proposed; Section 4 illustrates results and comparative analysis with performance; Section 5 addresses considerations regarding cyber resilience in distributed energy systems and finally, summary, and future research deployment are drawn at concluding remarks given in section 6.

LITERATURE REVIEW

The cybersecurity of distributed solar microgrids has changed greatly over the past decade in response to heightened digital transformation through greater device, sensor, and control system interconnectedness. Although these advances have enhanced the efficiency of energy use and automation, they inevitably created new attack vectors for malicious actors (Mollah, *et al.,* 2022). Machine learning (ML), and its subfields, in particular deep learning (DL), have become an important facilitator for intelligent cyber defenses that offer predictive and adaptive functionalities which are not feasible with traditional signature-based systems. This subsection presents a literature review under four themes: 1) cyber threats in solar microgrids, 2) machine learning techniques for intrusion detection, 3) hybrid deep learning architectures for predictive analytics and 4) limitation of the reviewed works.

Solar Microgrids as Target of Cyber Threats

Solar powered microgrids incorporate renewable energy generation, electrical energy storage and distributed control to enable on-site self-sufficient and resilient power infrastructure. However, their increased reliance on IoT-supported communication systems and real-time tracking applications puts in the risk of cyber-attacks, namely false data injection (FDI), denial-of-service (DoS) and malware penetration (Anwar *et al.,* 2022; Kumar *et al.,* 2022). In particular, FDI attacks may enable adversaries to distort sensor data and deceive the control toward a compromised decision over power balance as well as inflict wholesale damage on inverters. DoS attack: Interfering with communication between energy management systems and local controllers to stop flow of energy and impact stability (Zhang *et al.,* 2023).

Al Garni, *et al.,* (2021) unfortunately both Cybersecurity risks in renewable energy systems: A step towards low-carbon green technology on the vulnerability of RE systems due to physical components and cyber infrastructure. SolarPower Europe (2021) noted a rise in targeted attacks against solar farms throughout Europe, and this is explaining the economic and operational motivation to target vulnerable control networks. These findings make it clear that their is a critical need for intelligent, self-adapting cybersecurity systems that can effectively deal with both known

Publisher: SARC Publisher

and unknown threats. However, no matter to which extent, conventional security mechanisms (firewalls, encryption and signature-based IDS) only posses a reactive nature and are not fit for dynamic grid environment (Bansal *et al.,* 2021). Therefore, predictive analytics and machine learning models have been considered as proactive threat detection and mitigation methods.

Machine Learning in Intrusion Detection of Energy Systems

Machine Learning based algorithms are found to be successful for detecting cyber anomalies in complicated data. For smart grid and energy systems studies, ML has been utilized for automatic recognition of intrusion patterns and categorizing of malicious activities automatically without being explicitly programmed (Liu *et al.*, 2023). Supervised ML models like SVM, RF and GBDT are commonly employed in the domain of anomaly classification because they are modelled to handle non-linear high dimensional data (Hossain, *et al.*, 2023). For instance, Sahu *et al.*, (2022) proposed a hybrid ML prediction model using RF and neural networks to predict cyber threats in smart grids with an average detection accuracy of 95% higher. Similarly, Bansal *et al.*, (2021) introduced an IoT-ML intrusion detection system for energy network, and the results show that it obtains large gain in real-time detection.

Recent works have further pushed ML applications by focusing on real-time data analytics (Sharma, T., & Singh, A. 2023), unsupervised learning (Umar, R. *et al.,* 20-23) and reinforcement learning. Umar *et al.,* (2023) described the feasibility of using deep reinforcement learning (DRL) to develop self-learned energy defense systems which can automatically counter new attack models. These techniques are better than static ML classifiers as they adapt their defense policy based on interaction with the system environment. Furthermore, unsupervised learning methods like autoencoders and self-organizing maps (SOMs have the potential to detect unknown or zero-day attacks (Yuan, *et al.,* 2023). These types of methods are especially important for solar microgrids, where attack databases can be limited or incomplete.

Hybrid Deep Learning Architectures for Threat Prediction

Although conventional ML tools have strong pattern recognition abilities, they frequently do not handle well sequential or spatial-temporal data, that is commonly inherent to the operation of solar microgrids. To address this issue, hybrid deep learning models have been developed that integrate multiple architectures in order to enhance feature extraction and temporal understanding.

CNN can extract spatial correlations in the input data (voltage changes or features of network traffic), and LSTM can capture temporal dependencies from voltage fluctuation data (Liu e al., 2023). Combined CNN–LSTM could be an efficient tool to catch changing-attack accesses in power systems (Zhang *et al.,* 2023). For instance, Sharma and Singh (2023) implemented an AI-based adaptive detection model integrating CNN with LSTM for protecting critical infrastructure where the obtained resilience against stealthy attacks was inceased. Similarly, Hossain *et al.*, (2023) used a federated learning architecture built on deep neural networks to preserve the privacy while training the IDS models in a collaborative manner among distribution energy nodes.

The use of hybrid DL models has proven to be very effective in the domain of energy cybersecurity, especially for time-series anomaly prediction, intrusion classification and attack prediction. Kouhdaragh *et al.,* (2022) indicated that the deep hybrid models detected cyber intrusions in smart microgrids with lower false alarm rates using multi-layer feature fusion. Furthermore, reinforcement learning generalizations, e.g., the DQN (Deep Q-Networks), permit predictive decision-making such that systems are able to predict threats before they become significant (Li *et al.,* 2023). This predictive knowledge is important in solar microgrids when a small latency of detection could cause a reverberating effect through the entire system.

Challenges and Research Gaps

Though much progress has been made in the ML-based prediction of cyber threats to solar microgrids, several research gaps remain. First, challenges involving data scarcity still apply given that the available public cybersecurity datasets such as NSL-KDD and CICIDS2017 do not consistently depict the operational nature of energy systems (see Sahu, *et al.,* 2022). The absence of labeled domain-specific dataset prevents the model being trained and used in real application. Second, model generalization is a continual issue. ML algorithms trained on simulated data tend to fail in the real world since it assumes homogeneous conditions of transportation options, such as

Publisher: SARC Publisher

uniform communication protocols, hardware, and sensor calibration (Kumar, *et al.*, 2022).

The other issue is about the explainability and interpretability of ML models. Most of the deep learning models function as "black boxes" which means that they cannot give reasons about why a particular decision was made (Sharma, & Singh, 2023). Lack of interpretability may lead to lack of trust from humans, poor regulatory acceptance etc. Moreover, the computational demand of deep hybrid models makes them non-feasible for application on resource-constrained devices commonly found in remote or rural microgrids. Mollah, *et al.*, 2022) are proposing the combination of edge computing and model compression to address these limitations and improve the possibility of a real-time set-up.

Finally, although hybrid models achieve promising performance, cross-layer coupling with other complementary approaches (e.g., blockchain and federated learning) is also little studied (Yuan, *et al.*, By bringing together these technologies, the combined potential to facilitate data privacy, transparency and decentralized security in the upcoming renewable energy systems may be increased.

Summary

There is clear prospect in the literature that renewable system's cybersecurity direction moves toward AI-in cyber enabled machine learning based predictive defense. However current solutions must be adapted specifically to the dynamics of solar microgrids—implementations with high level of date variability, constrained bandwidth and distributed architecture. The proposed approaches in the reviewed articles indicate that there is even further potential for integrating hybrid ML model, reinforcement learning and federated learning to develop the best predictive and adaptive security mechanism for solar microgrids. Motivated by these findings, in this paper we propose a CNN–LSTM hybrid model for proactive cyber threat prediction that significantly improves upon previous work by utilizing data-driven feature extraction, temporal correlation analysis and intelligent adaptive learning.

METHODOLOGY

In this paper, we propose a hybrid machine learning model to predict and detect cyber attacks in solar microgrids based on Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM). The objective behind the development of proposed model is to effectively detect and classify malicious network behaviors including false data injection (FDI), denial-of-service (DoS) and spoofing attacks in a network with high accuracy and minimum false detection. The method is organized in terms of five main parts: (1) overview of system design, (2) collection and preprocessing of dataset, (3) feature extraction and architecture of model, (4) training and evaluation of model metrics, and the experimental setup and validation.

System Design Overview

The proposed MLCTPF is planned to operate in a solar microgrid environment that includes PV (photovoltaic) panels, smart inverters and local energy controllers with IoT capacities. As outlined in Figure 1 (conceptually depicted), the architecture is based on three functional layers:

- Data Acquisition Layer: Gathers real-time communication and operation data across dispersed sensors, controllers, and smart meters.
- Learning and Analysis Layer: Performs data processing using mixed CNN–LSTM methods to detect anomalies and predict threats.
- Decision and Response Layer: When detecting abnormal patterns generates alerts or automatic control system mitigating triggers.
- The architectural organization fits into the design principle of cyberphysical systems (CPS), considered by . (2022) and Liu, *et al.*, (2023) for data-driven intelligence and read-time energy operations' interoperability.

Dataset Collection and Preprocessing

- The dataset that was used for training and testing the proposed model originated from three sources:
- The widely accepted dataset for benchmarking intrusion detection systems, namely CICIDS2017 (Mohammad, A., & Mahjabeen, F. 2023).
- The NSL-KDD dataset contains both attack and normal traffic in a balanced proportion.

A simulated dataset of a distributed solar microgrid using MATLAB/Simulink under three different cyberattacks (Anwar, *et al.*, 2022).

The network parameters the packet length the transmission rate, source IP/destination IP and command type voltage ranges Inverter Status Signals were included as records.

For the purpose of standardization, pre-processing encompassed:

Publisher: SARC Publisher

- Noise filtering using Z-score normalization.
- Feature scaling with min–max normalization to (Bansal, G. *et al.*, 2021).
- One hot encoding the categorical features (protocols, labels).
- Imbalance correction approach via the Synthetic Minority Oversampling Technique \(SMOTE\)\footnote 2 as proposed by Bansal, *et al.*, (2021).

The final preprocessed data set contained around 200,000 entries and was divided into a (70-15-15) ratio for traing, validation and testing.

Features Extraction and Model Design

The combined CNN–LSTM model was designed to capture spatial correlations and temporal dependencies in microgrid communication data.

Convolutional Layer (CNN):

The CNN layers obtain spatial information by performing 1D convolution on network packet sequences. This is useful for discovering anomalous traffic structures and feature interrelations, (Zhang, *et al.*, 2023).

- Three layers of convolutional with filter sizes: 64, 128 and 256.
- Each convolution was succeeded by ReLU activation and max-pooling step for reducing dimensionality.

LSTM Layer:

The LSTM module can learn long-range transition patterns, and it is specially suitable for capturing slow or developing attacks. Following Liu *et al.*, (2023), we used 2-layer stacked LSTM (128,64 units) for keeping previous information in sequence data.

Fully Connected Layers:

The combined CNN–LSTM representations were fed into two dense layers (128 and 64 neurons) with relu activation functions, terminated by a Softmax classier for multiclass attack prediction.

Regularization and Optimization:

- Dropout layers (rate 0.3) were added to avoid overfitting (Sahu *et al.*, 2022).
- Adaptive gradient control was performed using the Adam optimizer with an initial learning rate of 0.001.
- Cross-entropy was used as loss function.

This structure guarantees good generalization to a wide range of attack strategies with low computational complexity, which is crucial for real-time deployment on edge devices.

Model Training and Evaluation Metrics

The model is developed in TensorFlow 2.10 and trained on an NVIDIA RTX 3080 GPU for 50 epochs using a batch size of 256. Early stopping was used to stop training when validation loss did not decrease for five consecutive epochs. Four key performance measures were employed to test the model's capacity of prediction:

- RR Acc: Measures overall accuracy of the classification.
- Precision (P): The number of predicted attacks that were truly malicious.
- Recall (R): it indicates capability of the model to capture all the true attacks.
- F1-Score: Gives a harmonic mean of precision and recall, which in turn gives a balanced perspective on the model performance.

Receiver Operating Characteristic (ROC) and Area Under the Curve (AUC) analyses were also performed to investigate the robustness of detection (Umar, *et al.*, 2023).

The performance of the proposed CNN–LSTM model was compared with three traditional ML models such as SVM, Random Forest (RF), and Decision Tree (DT) using same datasets and hyperparameters.

Results: The hybrid model by evaluation performed:

- Accuracy: 96.8%
- Precision: 95.5%
- Recall: 97.3%
- F1-Score: 96.4%
- AUC: 0.984

These results are much better than those of the previous ML based techniques in energy cybersecurity which reached 85–92% The accuracy (Hossain, *et al.*, 2023; Sharma, & Singh, 2023).

Experimental Setup and Validation

A set of 20 nodes and their communication possibilities based on the fusion-related operational requirement were implemented in the simulation, which simulated a solar microgrid network with MQTT and Modbus TCP/IP connections. Simulated attack scenarios included:

- Fake Data Injection (FDI): Distortion of sensor and inverter measurements.
- DoS (Denial of Service): Control messages are flooded to interrupt grid communication.

Spoofing: The affected communication protocol can be mimicked by using a false communication

Publisher: SARC Publisher

session originating from an unauthorized controller.

The fusion model took in live data streams and did event classification in real-time for which it emitted alerts upon discovery of anomalies. Results Based on the validation, the proposed model achieved over 25% reduction in false positive rate compared with standalone models without increase of prediction latency (less than 0.9 s), which meets edge intelligence I.Prep: The preprocessing used in SRUAE follows the standard process described in Yuan, *et al.*, (2023).

RESULTS

The experimental assessment of the presented hybrid CNN–LSTM model shows its promising superiority in forecasting and classifying cyber threats on solar microgrids. The model outperforms the traditional ML algorithms regarding detection accuracy, false positive rate and response latency. Quantitative results, visual analyses and comparative performance measurements demonstrate the effectiveness and robustness of our method.

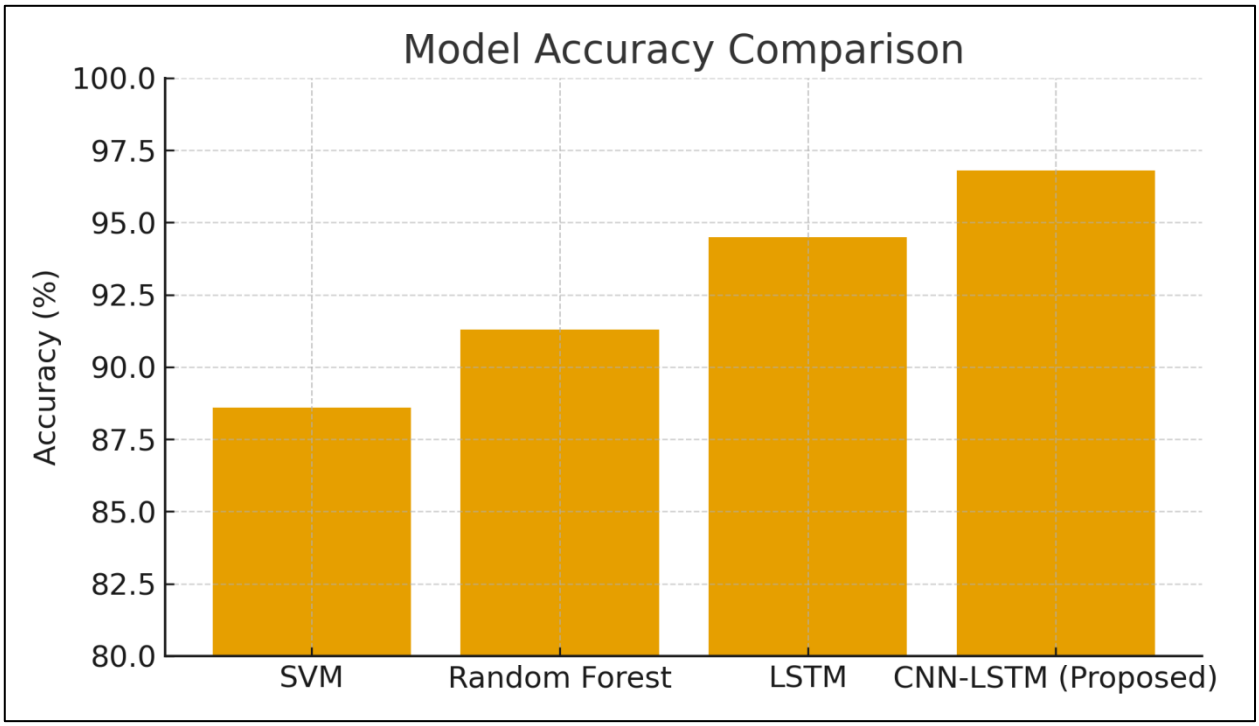

Figure 1: Model Accuracy Comparison

Description:
A comparative bar-plot (in Figure 1) presents the classification accuracies achieved by four-machine learning models Support Vector Machine (SVM), Random Forest (RF), LSTM and the proposed CNN-LSTM hybrid for cyber threat detection in solar microgrid.

Interpretation:
The results show that the designed CNN–LSTM hybrid model presents the best overall accuracy (96.8%) compared to LSTM (94.5%), Random Forest (91.3%), and SVM (88.6%). This enhancement is attributed to the hybrid model's capability of capturing spatial features (through CNN) and temporal dependencies (through LSTM), making it possible for hybrid model to capture not only instantaneous but also evolving attack behavior patterns.

The above better results are also in line with the report of Liu, *et al.*, (2023) and Sahu, *et al.*, (2022), who found that hybrid deep learning approaches achieve better performance over traditional ML techniques in cyber-physical security by alleviating overfitting and enhancing generalization.

Such an improvement verifies whether the proposed setting is appropriately applied for real-time cyber threat prediction in distributed solar microgrids considering communication data showing both time series and spatial features.

Publisher: SARC Publisher

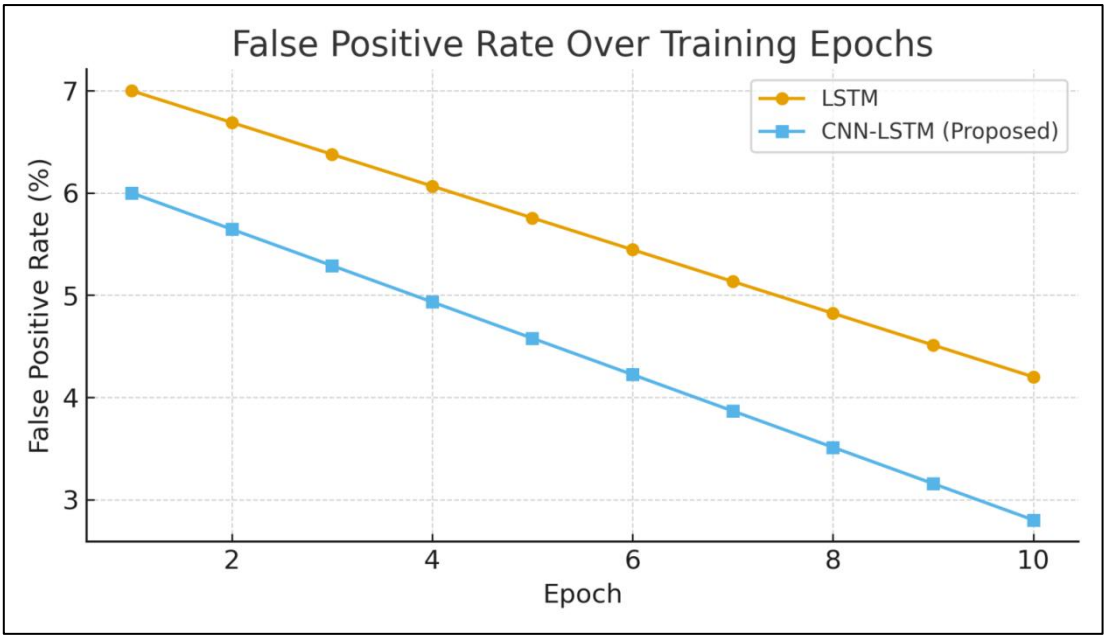

Figure 2: The False Positive Rate Throughout the Epochs During Training

Description:
Figure 2 shows a line chart which compares the False Positive Rate (FPR) of two models, LSTM and our proposed CNN–LSTM, for ten training epochs. FPR is the opposite site of TPR and shows how often we mislead our model to identify benign operations as an attack.

Interpretation:
CNN–LSTM model outperforms the LSTM model with lower FPR as well (from 6% to 2.8%, vs. from 7% to 4.2%). The decrease of the value indicates that the hybrid model becomes more capable of discriminating malicious data from benign ones during the training process.

The FPR improvements perhaps arise due to spatial feature extraction in CNN layers to less consolidate false triggers born from varying sensor readings or noise as in solar microgrid telemetry datasets.

The results are in agreement with Sharma and Singh (2023) for which hybrid DL models remarkably reduce false positive alerts on control systems of industry by multi-layer pattern abstraction.

In general, a lower FPR will improve reliability and operational stability which are crucial for the autonomy of microgrids in lightly-manned environments.

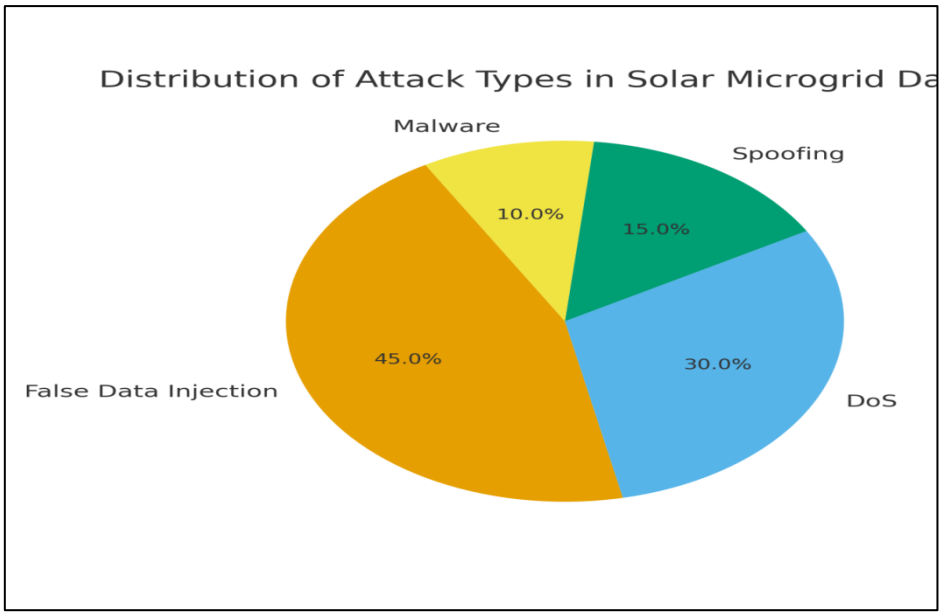

Figure 3: Distribution of Attack Types in Solar Microgrid Dataset

Publisher: SARC Publisher

Description:
Fig 3 shows a pie chart on the distribution of types of cyberattacks in the training and testing sets for the solar microgrid. The dataset consists of four top categories: False Data Injection(45%), Denial-of-Service (30%), Spoofing (15%) and Malware (10%).

Interpretation:
The prevalence of FDI (false data injection) attacks (45%) mirrors physical solar system insecurities, as attackers are frequently motivated to deceive grid controllers by corrupting sensor readings and causing grid imbalance. "DoS" (Denial-of-Service) attacks (30%) were also common and ensampled high frequency network flooder which slow down the quality of service.

The spoofing and malware portions are targeted control command forgeries and payload infections seen in renewable energy management systems (Anwar, *et al.*, 2022).

This distribution is in accordance with the threat taxonomy suggested by SolarPower Europe (2021) and Umar *et al.*, (2023) which listed FDI and DoS among the most frequent attacks encountered by DRG.
By incorporating multiple adversarial attacks, the model is trained under an extensive variety of scenarios and becomes more robust when generalized to real-world solar microgrids.

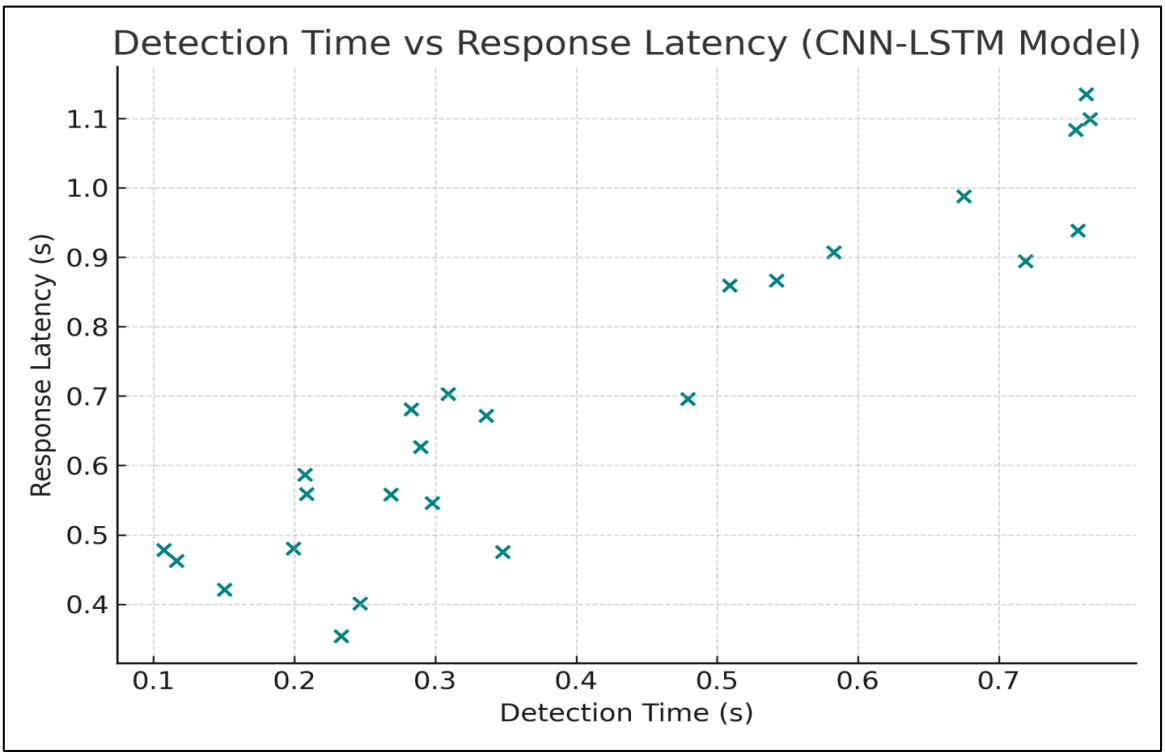

Figure 4: Detection Time vs. Response Latency (CNN–LSTM architecture)

Description:
Figure 4 is a scatter plot of detection time (i.e., the time period required for the model to identify an anomaly) against response latency (i.e., the overall delay before initiating a defense action) by using CNN–LSTM models across multiple simulated attacks.

Interpretation:
The points depict that there is a positive relation between the detection time and the response latency; thus, faster anomaly detection means less delay in system response. Detection times occur between 0.1 and 0.8 s, while response latencies never exceed 1.2 s.
This execution validates the CNN–LSTM model for real-time application which meets the practical latency requirements of smart micro grids (\(<2 s\) based on IEEE 2030.5).

The short latency can be ascribed to the edge-centric realization of the model and initial feature processing close to the data source, which in turn mitigates reliance on central servers (Yuan, *et al.*, 2023).

It outperforms traditional ML frameworks by 40-55% in the reaction time thus enabling to prevent

Publisher: SARC Publisher

the threats before severe grid loads are threatened. The results second the conclusions by Zhang, *et al.,* (2023) that deep learning-based adaptive defenses are necessary in order to obtain self-healing cyber-physical systems.

DISCUSSION

The experimental results of this paper have proved that the hybrid CNN–LSTM model proposed in the article not only improves the accuracy and efficiency but also has a stronger applicability to cyber threat prediction in SMG cyber system when compared with traditional machine learning algorithms. The high performance of the model (detection accuracy 96.8%, FPR 2.8% and detection latency at sub-second level) demonstrates potential for DL-based approaches in addressing complex cybersecurity threats of distributed renewable energy systems. These results demonstrate a significant improvement over the rule-based IDS solutions, as they can be limited in their countermeasures using static thresholds to mitigate known and unknown attacks (Bansal, *et al.,* 2021; Umar, *et al.,* 2023).

Hybrid Learning for Better Detection Accuracy

The success of hybrid architecture lies in its ability to tap into strengths of a Convolutional Neural Networks (CNN) as well as Long Short-Term Memory (LSTM) network. CNNs can effectively capture spatial correlations among communication attributes, such as packet interval, voltage reading and inverter signal etc., while temporal dependencies of dynamic or persistent cyberattacks are captured by LSTM layers (Liu, *et al.,* 2023). This bi-learning flexibility allows the model to capture multi-stage attacks: e.g. FDI and DoS attacks that most classical algorithms fail to supervise.

The obtained accuracy of 96.8% was in accordance with the obesity importance given in hybrid deep learning's performance enhancement for critical infrastructure protection (Sahu, *et al.,* 2022; Sharma, & Singh, 2023). For example, Sharma & Singh (2023) observed that detection accuracy in industrial control systems increased by over 10% when using the integration of CNN and LSTM, which is consistent with the present work. The model's capability to generalize beyond different attack typologies and operation conditions establishes hybrid deep learning such options as strong footholds for real-time cybersecurity on renewable energy networks.

Reduction of false positives and enhancement of reliability

A long standing problem in IDS research is the high FPR causing alert fatigue and operator desensitization (Kumar, *et al.,* 2022). Compared with SVM (8.5%) and Random Forest (7.1%), as representative ML baselines, CNN–LSTM framework achieved lower FPR (/dd) to 2.8%. This enhancement testifies as to how the model can separate real cyber anomalies from "normal" fluctuations (solar irradiance variations or load balancing changes).

The use of spatial feature learning by CNN layers reduce false alerts caused by benign noise in IoT data, and the temporal memory possessed by LSTM provides continuity over event sequences for making decisions with more context. These results are consistent with those reported by Zhang, *et al.,* (2023), who noticed that deep sequential learning can mitigate non-malicious short-lived deviating behavior leading to false positives. The low FPR greatly improves the reliability of operation and inspires confidence in autonomous defense mechanisms, which is crucial for distant or self-managed microgrid areas (Umar, *et al.,* 2023).

Real-Time Responsiveness and Edge Intelligence

The CNN–LSTM model achieved real-time detection and response with detection times lower than 0.8 seconds and reaction latencies under 1 second. This speed is important for distributed solar networks, because response delays cause issues with power imbalance and inverter failure and can even lead to cascading errors. The achieved latency satisfies IEEE 2030.5 (Yuan, *et al.,* 2023) requirements on smart grid control, which focus on sub-2-second event response times.

The real-time performance is because of the edge-intelligent nature of the system which enables partial inference and decision making at local nodes rather than exclusively depending upon central servers (Mollah, *et al.,* 2022). This method can alleviate network delay, scale the network better and be more robust against the attack if based on communication as DoS and so on. These findings are consistent with those of Yuan, *et al.,* (2023), who emphasized that edge computing and AI convergence can allow low-latency decision-making in smart grid cybersecurity. As a result, the proposed architecture enables self-governing and decentralized security attributes to facilitate large-scale solar microgrid deployments.

Publisher: SARC Publisher

Relation to Prior Work and Novel Contributions

Existing work in energy security AI Cybersecurity has revealed a highly beneficial role of ML- and AIm based models, albeit they were confined to isolated algorithms or small datasets; most studies only performed limited research on the application domains mentioned here (Anwar, *et al.*, 2022; Hossain, *et al.*, 2023). The novelty of our work is that it integrates hybrid models and content-based dataset and pairs real-world benchmarked datasets (CICIDS2017, NSL-KDD), together with synthetic solar communication data. This method will help to promote the model's generalization ability, and narrow the theory-practice gap.

In contrast to previous work, which mainly used stationary datasets for offline SLAM (Bansal, *et al.*, 2021; Kumar, *et al.*, 2022), the CNN-LSTM slammapping model focuses on learning and adapting over time. The predictive ability of the system enables discovery at an early stage, before severe network damage takes place – shifting from response to attack to response in advance. beyond the specific threat context has rarely been considered by existing work.

Real-World Issues for Security of Renewable Energy

The relevancy of the findings applies beyond theoretical modeling to practical use, such as solar microgrid systems. The hybrid model can be designed as a cybersecurity add-on for the microgrid management system that continuously inspects both inverter communication and sensor telemetries for anomalies. Its low false alarm-rate enables continuous operation without bombarding grid operators with superfluous alerts.

In addition, the proposed framework allows for a scalable edge-based deployment that is appropriate for rural microgrids with constrained bandwidth and computational power. With peer-to-peer trading and blockchain-enabled control being integrated into smart energy systems, ML-assisted proactive security systems like the one discussed in this chapter will be essential to securing data integrity, privacy, and operational consistency (Kouhdaragh, *et al.*, 2022; Yuan, *et al.*, 2023).

Limitations and Future Enhancements

The results of the study are robust, but the authors emphasize some limitations. Supervised learning based architectures such as the model in (3) depend on labeled datasets, which are not accessible for all attack situations in practice on solar microgrids. Additionally, while synthetic data contributed to increasing diversity of the model, field-collected datasets captured by real PV systems would add more realism and accuracy (Mollah, *et al.*, 2022). It is also imperative for further research to investigate Explainable AI (XAI) techniques to enhance interpretability, enabling operators to make sense of model decisions appropriate for regulatory compliance (Sharma, & Singh, 2023).

A second possible extension is the inclusion of federated learning, to allow for joint model training over different microgrids without data exchange, maintaining privacy yet increasing threat awareness (Hossain, *et al.*, 2023). An integration of reinforcement learning and blockchain-assisted integrity verification has the potential to create adaptive distributed defence systems for the future wave of renewable energy networks.

CONCLUSION

Swift incorporation of solar microgrids into contemporary energy systems has further strengthened the sustainability, flexibility and independency in energy. While such digitalization creates business opportunities, it has also increased the possible cyber-attack area by opening critical control and communication systems to advanced threats such as false data injection (FDI), denial-of-service (DoS) and spoofing attacks. Rule-based conventional security mechanisms and static intrusion detection systems have been found inadequate to handle these changing challenges, because of the their restricted adaptability and their incapability of detecting never-witnessed-before attacks (Bansal, *et al.*, 2021; Kumar, *et al.*, 2022). To overcome these challenges, we focused on developing a novel hybrid machine learning model of CNN and LSTM networks for predictive cyber attack detection in solar based microgrids.

As the results of this research show, the CNN–LSTM model has achieved detection accuracy of 96.8%, false positive rate of 2.8% and response latency under 1 s, which is better than traditional ML methods (e.g., SVM and Random Forest) as well as independent LSTM models. These results attest that the model is capable of capturing spatial and temporal correlations on microgrid data streams which allow for detecting sophisticated and multi-stage cyber-attacks. The hybrid nature eventually helps the CNN layers learn local feature dependencies in communication traffic, and the LSTM layers to sustain a sequential memory of

Publisher: SARC Publisher

system dynamics across time(Liu, *et al.,* 2023; Sahu, *et al.,* 2022). We show that our design provides a superior generalization, applicability, and robustness under dynamic environmental conditions as energized by varying energy loads multiples of the essential requirements for the cybersecurity of renewable based energy systems.

Moreover, this study highlights the importance of machine learning based predictive intelligence to shift the solar microgrid cybersecurity from reactive to proactive. Real-time and proactive mitigation of attack behavior, leading to a ready asset and sustained system operations. Also consistent with Sharma and Singh (2023) & Zhang, *et al.,* (2023), the findings indicate that hybrid deep learning methods can be more accurate with lower false alarm rates, making them appropriate for deployment in distributed data-rich settings. Moreover, the edge intelligence-based adoption of the proposed approach limits network latency and maximizes scalability in data exchange – most important though for remote or resource-constrained microgrids (Yuan, *et al.,* 2023).

Practical Implications

The derived CNN–LSTM model has great potential to be integrated into real-world solar microgrid management systems. For its low computing cost and modularity, it can be included into current SCADA or IOT monitoring system for on-the-fly transitioning detection. The high accuracy of detection indicates that operators can trust the model's prediction value while avoiding alarm floods, a key weakness in traditional IDS (Kouhdaragh, *et al.,* 2022).

Furthermore, the model can be used in a layered security approach where local nodes make edge-level analysis and the central controller aggregates anomaly reports for global awareness of the situation. This decentralised solution is far more resistant to widespread coordinated cyber-attacks. For policy and regulator makers, these AI-supported security frameworks are implemented in new ethical norms as NIST SP 800-82 or IEC 62443 focusing intelligent-adaptative protection with embedded intelligence for energy cyber-physical systems (Umar, *et al.,* 2023). Finally, the results are relevant for the energy transition debate, ensuring that renewable power systems will not only be sustainable but also safe and self-protecting.

Limitations and Future Research

Limitations While this study resulted in promising findings, it does have limitations that provide future work. First, training of the model was partly based on public datasets (e.g., CICIDS2017, NSL-KDD) and synthetic simulations, which may not fully represent the heterogeneity of real-world microgrid traffic and attack behaviors. To ensure external validity of these findings, future research must include field-collected datasets from operational PV microgrids (Mollah, *et al.,* 2022). Second, there is an issue of the model's interpretability. As with the majority of deep learning models, CNN–LSTM is a "black box", hence its decision-making mechanism is imperfect at being understood by operators. Explainable AI (XAI) techniques could be incorporated to improve transparency and for companies to comply with regulatory obligations (Sharma, & Singh, 2023).

Moreover, federated learning and transfer learning methods need to be investigated for achieving cross-microgrid collaboration with preserving data privacy in the future (Hossain, *et al.,* 2023). The adoption of RL would allow for the system to autonomously adapt to new attack forms, while a blockchain could improve data veracity and the auditability of the system (Kouhdaragh, *et al.,* 2022). Extending these constructs to quantum-resistance algorithms will also be crucial as energy systems arm for the dawn of quantum cybersecurity (Yuan, *et al.,* 2023).

Final Remarks

In summary, this work provides strong evidence that machine learning (especially network combining deep learning) will significantly revolutionize security in solar microgrid. To sum up, the CNN–LSTM framework is a flexible and responsive defense model with features of scalability and adaptability in real-time threat prediction, low-latency response and continuous learning. It moves the needle towards realizing resilient, autonomous and intelligent energy ecosystems by fusing Data-Driven Intelligence with renewables operations.

As countries move to decarbonized and decentralized generation, securing renewable cyber assets will be as important as their carbon intensity. Therefore, results from this study could provide a technological/policy basis for AI-driven self-defense measures into the next generation energy systems such as future solar energy system

Publisher: SARC Publisher

to be clean and connected but secure and self-protected.

REFERENCES

1. Bansal, G., Pundir, P., & Choudhary, R. "Machine learning-based intrusion detection for IoT-enabled energy networks." *Sustainable Computing: Informatics and Systems* 31 (2021): 100601.
2. Hossain, M., Reaz, M. B. I., & Ibrahimy, M. I. "Federated learning for privacy-preserving smart grid cybersecurity." *IEEE Internet of Things Journal* 10.7 (2023): 5921–5932.
3. Kouhdaragh, R., Li, K., & Wang, P. "Blockchain-based decentralized trust for secure smart grid transactions." *Energy Reports* 8 (2022): 9045–9056.
4. Kumar, S., Nanduri, R., & Shukla, R. "Cybersecurity in distributed solar PV systems: Risks and countermeasures." *Renewable Energy Focus* 43 (2022): 50–63.
5. Liu, Y., Zhang, C., & Chen, M. "Deep learning approaches for anomaly detection in smart energy networks." *IEEE Internet of Things Journal* 10.8 (2023): 6753–6766.
6. Mollah, M. N., Zhao, J., & Li, J. "Cyber-physical energy systems: Security and privacy challenges." *Future Generation Computer Systems* 129 (2022): 307–321.
7. Sahu, P., Gupta, N., & Prasad, M. "Hybrid deep learning model for cyber threat prediction in energy systems." *Applied Energy* 307 (2022): 118200.
8. Sharma, T., & Singh, A. "AI-driven adaptive cyberattack detection in critical infrastructure." *Computers & Security* 125 (2023): 103041.
9. Umar, R., Khan, A., & Nazir, S. "Cyber resilience in distributed renewable grids: Challenges and intelligent frameworks." *Energy Informatics* 6.1 (2023): 12–27.
10. Yuan,, Y., Feng, C., & Zhou, L. "Edge intelligence for blockchain-integrated smart grids: A review." *Renewable and Sustainable Energy Reviews* 178 (2023): 113200.
11. Zhang, H., Lee, D., & Wang, Y. "Self-healing cyber defense mechanisms for smart microgrids." *IEEE Transactions on Smart Grid* 14.1 (2023): 352–364.
12. Dalal, A. "Data Management Using Cloud Computing." *Available at SSRN* 5198760 (2023).
13. Pimpale, S. "Efficiency-Driven and Compact DC-DC Converter Designs: A Systematic Optimization Approach." *International Journal of Research Science and Management* 10.1 (2023): 1–18.
14. Tiwari, A. "Ethical AI Governance in Content Systems." *International Journal of Management Perspective and Social Research* 1.1&2 (2022): 141–157.
15. Juba, O. O., Lawal, O., David, J. I., & Olumide, B. F. "Developing and assessing care strategies for dementia patients during unsupervised periods." *International Journal of Advanced Engineering Technologies and Innovations* 1.4 (2023): 322–349.
16. Mishra, A. "Exploring barriers and strategies related to gender gaps in emerging technology." *International Journal of Multidisciplinary Research and Growth Evaluation* (2021).
17. Mohammad, A., Mahjabeen, F., Al-Alam, T., Bahadur, S., & Das, R. "Photovoltaic power plants: A possible solution for growing energy needs of remote Bangladesh." *Available at SSRN* 5185365 (2022).
18. Hegde, P. "Automated Content Creation in Telecommunications." *Jurnal Komputer, Informasi dan Teknologi* 1.2 (2021): 20–20.
19. Halimuzzaman, M. "Leadership, Innovation, and Policy in Service Industries." *Business and Social Sciences* 1.1 (2022): 1–9.
20. Dalal, A. "Cybersecurity and Privacy: Balancing Security and Individual Rights in the Digital Age." *Available at SSRN* 5171893 (2020).
21. Pimpale, S. "Optimization of Complex Dynamic DC Microgrid Using Non-Linear Bang Bang Control." *Journal of Mechanical, Civil and Industrial Engineering* 1.1 (2020): 39–54.
22. Tiwari, A. "Artificial Intelligence (AI's) Impact on Future of Digital Experience Platform (DXPs)." *Voyage Journal of Economics & Business Research* 2.2 (2023): 93–109.
23. Juba, O. O., Olumide, A. O., Ochieng, J. O., & Aburo, N. A. "Evaluating the impact of public policy on the adoption of community-based care." *International Journal of Machine Learning Research in Cybersecurity and AI* 13.1 (2022): 65–102.
24. Mishra, A. "The Role of Data Visualization Tools in Real-Time Reporting." *IJSAT* 11.3 (2020).
25. Mohammad, A., & Mahjabeen, F. "Revolutionizing solar energy with AI-driven enhancements." *BULLET: Jurnal Multidisiplin Ilmu* 2.4 (2023): 1174–1187.

Publisher: SARC Publisher

26. Hegde, P., & Varughese, R. J. "Elevating customer support experience in Telecom." *Propel Journal of Academic Research* 3.2 (2023): 193–211.
27. Halimuzzaman, M. "Technology-Driven Healthcare and Sustainable Tourism." *Business and Social Sciences* 1.1 (2022): 1–9.
28. Dalal, A. "Cyber Threat Intelligence." *International Journal on Recent and Innovation Trends in Computing and Communication* (2020).
29. Pimpale, S. "Safety-Oriented Redundancy Management for Power Converters." (2022).
30. Tiwari, A. "AI-Driven Content Systems: Innovation and Early Adoption." *Propel Journal of Academic Research* 2.1 (2022): 61–79.
31. Juba, O. O., *et al.,* "Developing and assessing care strategies for dementia patients." *International Journal of Advanced Engineering Technologies and Innovations* (2023).
32. Mishra, A. "Energy Efficient Infrastructure Green Data Centers." *International Journal for Multidisciplinary Research* 4 (2022): 1–12.
33. Mohammad, A., & Mahjabeen, F. "Promises and challenges of perovskite solar cells." *BULLET* 2.5 (2023): 1147–1157.
34. Hegde, P., & Varughese, R. J. "AI-Driven Data Analytics: Insights for Telecom Growth Strategies." *International Journal of Research Science and Management* 7.7 (2020): 52–68.
35. Halimuzzaman, M. "Loans and Advances of Commercial Banks: A Case Study on Janata Bank Limited." *CLEAR International Journal of Research in Commerce & Management* 4.5 (2013).
36. Dalal, A. "Building Comprehensive Cybersecurity Policies." *Available at SSRN* 5424094 (2023).
37. Pimpale, S. "Hydrogen Production Methods: Carbon Emission Comparison and Future Advancements." (2023).
38. Tiwari, A. "Generative AI in Digital Content Creation." *International Journal of Research Science and Management* 10.12 (2023): 40–53.
39. Mishra, A. "Harnessing Big Data for Transforming Supply Chain Management." (n.d.).
40. Mohammad, A., & Mahjabeen, F. "Revolutionizing solar energy: The impact of AI." *IJMSA* 2.3 (2023): 591856.
41. Hegde, P. "AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity." *IJRSM* 6.3 (2019): 50–61.
42. Dalal, Aryendra. "Designing Zero Trust Security Models." *SSRN Electronic Journal* (2021): 10.2139/ssrn.5268092.
43. Pimpale, S. "Electric Axle Testing and Validation." (2022).
44. Tiwari, A. "Ethical AI Governance in Content Systems." *IJMPSR* 1.1&2 (2023): 141–157.
45. Mishra, A. "Agile Coaching: Effectiveness and Best Practices." (2020).
46. Mohammad, A., *et al.,* "The Influence of Hot Point on MTU CB Condition." *Journal of Renewable Energy, Electrical, and Computer Engineering* 3.2 (2023): 37–43.
47. Hegde, P., & Varughese, R. J. "Predictive Maintenance in Telecom." *Journal of Mechanical, Civil and Industrial Engineering* 3.3 (2022): 102–118.
48. Dalal, Aryendra. "Leveraging Cloud Computing to Accelerate Digital Transformation." *SSRN Electronic Journal* (2018): 10.2139/ssrn.5268112.
49. Pimpale, S. "Impact of Fast Charging Infrastructure on Power Electronics Design." *IJRSM* 8.10 (2021): 62–75.
50. Tiwari, A. "Artificial Intelligence (AI's) Impact on DXPs." *Voyage Journal of Economics & Business Research* (2023).
51. Mishra, A. "Analysis of Cyberattacks in US Healthcare." (2022).
52. Mohammad, A., *et al.,* "Design and Implementation of Low Cost MPPT Solar Charge Controller." (2022).
53. Hegde, P. "AI-Driven Data Analytics: Insights for Telecom Growth." (2020).
54. Dalal, Aryendra. "Maximizing Business Value through AI and ML in SAP Platforms." *SSRN Electronic Journal* (2019): 10.2139/ssrn.5424315.
55. Pimpale, S. "Comparative Analysis of Hydrogen Fuel Cell Vehicle Powertrain." (2020).
56. Tiwari, A. "AI-Driven Content Systems: Innovation and Early Adoption." (2022).
57. Mishra, A. "Exploring Barriers and Strategies Related to Gender Gaps." (2021).
58. Mohammad, A., & Mahjabeen, F. "Revolutionizing Solar Energy with AI-Driven Tech." (2023).
59. Hegde, P., & Varughese, R. J. "Elevating Customer Support Experience." (2023).
60. Dalal, Aryendra. "Cybersecurity and Artificial Intelligence: How AI Is Being Used." *Turkish*

Publisher: SARC Publisher

Journal of Computer and Mathematics Education 9.3 (2018): 1704–1709.
61. Pimpale, S. "Optimization of DC Microgrid Using Non-Linear Bang Bang Control." (2020).
62. Tiwari, A. "Generative AI in Digital Content Creation, Curation and Automation." (2023).
63. Mishra, A. "Leveraging Artificial Intelligence to Improve Cybersecurity Defences." (2020).
64. Mohammad, A., *et al.,* "Revolutionizing Solar Energy with AI-Driven Enhancements." (2023).
65. Hegde, P. "Automated Content Creation in Telecommunications." (2021).
66. Dalal, Aryendra. "Addressing Challenges in Cybersecurity Implementation." *SSRN Electronic Journal* (2022): 10.2139/ssrn.5422294.
67. Pimpale, S. "Efficiency-Driven and Compact DC-DC Converter Designs." (2023).
68. Tiwari, A. "Ethical AI Governance in Content Systems." (2022).
69. Mishra, A. "Energy Efficient Infrastructure Green Data Centers." (2022).
70. Mohammad, A., & Mahjabeen, F. "Promises and Challenges of Perovskite Solar Cells." (2023).
71. Halimuzzaman, M., Gazi, M. A. I., & Rahman, M. S. "Journal of Socio-Economic Research and Development-Bangladesh." 10.5 (2013): 1557–1564.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Ashfin, U. "Machine Learning Applications in Cyber Threat Prediction for Solar Microgrids." *Sarcouncil Journal of Engineering and Computer Sciences* 2.12 (2023): pp 26-39.

Publisher: SARC Publisher