computation

MDPI

Article

A Novel ConvXGBoost Method for Detection and Identification of Cyberattacks on Grid-Connected Photovoltaic (PV) Inverter System

Sai Nikhil Vodapally and Mohd. Hasan Ali *

Department of Electrical and Computer Engineering, The University of Memphis, Memphis, TN 38152, USA; snvdplly@memphis.edu

* Correspondence: mhali@memphis.edu

Abstract: The integration of solar Photovoltaic (PV) systems into the AC grid poses stability challenges, especially with increasing inverter-based resources. For an efficient operation of the system, smart grid-forming inverters need to communicate with the Supervisory Control and Data Acquisition (SCADA) system. However, Internet-of-Things devices that communicate with SCADA make these systems vulnerable. Though many researchers proposed Artificial-Intelligence-based detection strategies, identification of the location of the attack is not considered by these strategies. To overcome this drawback, this paper proposes a novel Convolution extreme gradient boosting (ConvXGBoost) method for not only detecting Denial of Service (DoS) and False Data Injection (FDI) attacks but also identifying the location and component of the system that was compromised. The proposed model is compared with the existing Convolution Neural Network (CNN) and decision tree (DT) strategies. Simulation results demonstrate the effectiveness of the proposed method for both the smart PV and PV fuel cell (PV-FC) systems. For example, the proposed model is efficient with an accuracy of 99.25% compared to the 97.76% of CNN and 99.12% of DT during a DoS attack on a smart PV system. Moreover, the proposed method can detect and identify the attack location faster than other models.

Keywords: smart grid; intrusion detection system (IDS); cyber-physical security; deep learning; CNN; decision tree

Academic Editors: Stefan Hensel, Marin B. Marinov, Malinka Ivanova, Maya Dimitrova and Hiroaki Wagatsuma

Received: 18 November 2024
Revised: 14 January 2025
Accepted: 24 January 2025
Published: 1 February 2025

Citation: Vodapally, S.N.; Ali, M.H. A Novel ConvXGBoost Method for Detection and Identification of Cyberattacks on Grid-Connected Photovoltaic (PV) Inverter System. *Computation* **2025**, *13*, 33. https://doi.org/10.3390/computation13020033

1. Introduction

Microgrids, becoming increasingly popular, employ Distributed Energy Resources (DERs), such as solar energy, as sources of electric power. The energy harnessed from these resources is integrated with the conventional/main electric grid through inverters, grid following or grid forming, to ensure reliability of the grid. These can be used either locally or in an off-grid electric network or can be used for feeding into a commercial electric grid [1]. Smart inverters are those that can operate autonomously and have adaptive features along with plug-and-play functions. These can ride through minor disturbances to voltage or frequency, directing the distributed system to stay online and respond to short-term events.

Even though smart inverters are developed to operate in decentralized mode, they require Internet of Things (IoT) devices to interact with other components of the microgrid along with the traditional grid. These IoT devices, employed for these systems, effectively monitor various parameters and transmit and receive information. When these devices are exposed to the Internet, they pose a potential threat to the smart grids by creating a

vulnerable point of entry for cyber-intrusions. 5G networks (fifth generation of cellular networks) can offer suitable services for real-time operations in a microgrid, especially for smart inverters [2]. Even though the usage of 5G for smart inverters offers a promising solution to overcome the limitations of conventional grids, the continuous data exchange between different components of the grid and the control panel makes them vulnerable to cyberattacks, thereby posing serious threats to the operation of smart grids [3]. Cyberattacks on the electric grids are directly or indirectly associated with destabilizing the grid. Most of these can be based on malware, unauthorized access or Denial of Service (DoS) attacks [4]. Cyberattacks on smart inverters can be problematic, as they can alter the function of the inverter which may lead to undesirable states of the electric grid [5].

Providing security against such cyberattacks for the inverters in the smart grids is the biggest challenge for the system operators [6]. Even though vulnerable components can be secured against such attacks, dynamic measures are needed to protect them. This is possible if and only if the nature/type of the cyberattack is identified correctly. In addition, the devices that are attacked are also to be identified along with the impact created. Several techniques have been found in the literature to identify the nature of cyberattacks in smart grids [7–18].

Artificial Intelligence (AI) can be employed to improve reliability of the smart grids. Even though different techniques are available, deep learning appears to be the most effective AI technique for protecting smart grids against cyberattacks. It was found to be better than conventional techniques like fuzzy logic, genetic algorithms and expert systems [19]. Employing deep learning techniques can help the system in automatic identification of the features of cyberattacks, besides detecting cyber intrusions and malware injections, thereby reducing the probability of cyberattacks on the power systems [20]. Convolutional Neural Networks (CNNs) and decision trees (DTs) are widely used machine learning models in detecting cyberattacks in smart grids.

CNNs, a classification of deep neural networks, have multiple convolutional, pooling and fully connected layers and can learn hierarchical representations from raw data. They perform very well in extracting the features from the data and are able to identify the anomalies in the data. These factors encouraged researchers to develop CNN-based detection strategies as discussed in Table 1. Though all the works presented in Table 1 on CNN-based detection strategies demonstrated their efficiency in detecting cyber-intrusions, none of the papers presented a means to identify the specific location of the attack. Moreover, the CNNs are prone to overfitting which can lead to biased predictions. On the other hand, DTs have a tree-like structure, are highly penetrable and so can capture nonlinear relationships between features and target variables [21,22]. This encouraged researchers to use the DT for the detection of cyberattacks as shown in Table 2. Though Table 2 presents the instances of DTs used for intrusion detection, DTs always fail to capture the complex relationships in the data. Moreover, DTs tend to have high variance, which makes them more sensitive to small variations in training data. These drawbacks of DTs are addressed by the XGBoost model. XGBoost, which stands for extreme gradient boosting, is a machine learning algorithm that is developed based on an ensemble of DT. It is a scalable, distributed gradient-boosted decision tree (GBDT). It was designed to efficiently train machine learning models. It is able to solve real-world scale problems using a minimal number of resources [23]. It employs a regularization technique to address overfitting, is less susceptible to noisy data and improves performance by reducing the bias and variance. Moreover, XGBoost is highly scalable and efficient and is capable of handling large datasets with millions of data samples and features. It also provides feature importance scores, a metric showing the contribution of each feature, which helps to identify the informative features.

Table 1. Researchers proposed CNN detection models.

Authors	Model Used	Attack Tested	Major Findings
Osman Boyaci et al. [7]	Chebyshev Graph Convolutional Networks (CGCN).	Data scale attacks and distribution-based attacks.	For large-scale AC power grids, CGCN can capture spatial correlations of power grid measurements in a better way than fully connected neural networks (FNN) and Recurrent Neural Networks (RNN) and has a higher detection rate.
Samson Ho et al. [8]	Novel Intrusion Detection System (IDS) based on CNN.	DoS, brute force and web attacks.	Higher detection rate and lowest False Alarm Rates when compared to hierarchical, Random Forest and Naive Bayes models.
Kang-Di Lu et al. [9]	Representation-Learning-Based CNN.	DoS, False Data Injection (FDI), jamming and hybrid attacks.	RL-CNN is superior to two compositional metric-learning-based multilabel detection methods and two manifold regularized discriminative feature section-based multilabel detection methods, i.e., KNN-COM, MLK-COM, MDFS-MLK and MDFS-CNN in terms of five performance indices.
Moataz Abdelkhalek et al. [10]	Supervised machine learning (ML)-based anomaly detection algorithm.	DoS, remote automated attacks, unauthorized remote hacking attacks, scanning, DER Stealth Modbus attacks.	ANN-based IDS achieve high detection accuracy of 98.4% and very low detection latency of 5 ms with high precision and recall.
Kübra Bitirgen et al. [11]	Particle Swarm Optimization (PSO)-based convolutional neural networks—long short-term memory (CNN-LSTM).	FDI, relay setting change attack, remote tripping command injection, short-circuit fault and line maintenance.	PSO-CNN-LSTM is a more robust detection method for data injection, remote tripping command injection, attack sub-type (command injection against a single relay) and relay setting change attacks.
Jiaying Mao et al. [12]	Unified CNN-LSTM.	DoS, FDI attacks.	CNN-LSTM successfully classifies cyberattacks of different targets and modes in inverter-based cyber-physical systems.
Basim Ahmad Alabsi et al. [13]	Dual Convolutional Neural Network (CNN-CNN).	DoS, DDoS, reconnaissance and information theft attacks.	Combination of two CNNs can effectively detect IoT attacks in IoT networks.
Guangdou Zhang et al. [14]	Deep Capsule Convolution Neural Network (DC-CNN).	DoS, FDI, replay attacks, time-delay attacks and deception attacks.	Significantly higher performance than other methods.

With the above background, this paper proposes the ConvXGBoost method which combines the capabilities of a CNN and the XGBoost algorithm. The proposed approach not only can detect the cyber-intrusion but also identify the specific location or the component under attack, thereby helping to effectively mitigate cyberattacks. This proposed methodology has the feature selection capability of the CNN model and the robustness and interpretability of the XGBoost model. A similar method was used in biometric identification and authentication [24] application. This method, when tested for breast cancer and Parkinson's datasets, was found to be accurate in comparison to traditional families of machine learning [25]. However, the proposed ConvXGBoost method has not been used in the case of the smart PV inverter. This fact demonstrates the novelty of this paper.

This proposed method is developed in Python 3.11 and evaluated in comparison with traditional CNN and DT models. Moreover, these developed models are imported into the MATLAB/Simulink environment and evaluated to see how fast these models can detect

cyber-intrusions in the simulation environment. The proposed model is developed and tested on the DoS and FDI attacks of the grid-connected smart solar PV inverter system. The DoS attack is relevantly easy to implement and is difficult to trace. This attack poses an immediate threat when implemented, and a slight delay caused by this attack can disrupt the entire connected system [26].

Table 2. DT detection models proposed by researchers.

Authors	Model Used	Attack Tested	Major Findings
Seyedeh Mahsan Taghavinejad et al. [15]	Hybrid DT.	DoS, Probe, R26, U2R attacks.	The combination of multiple decision trees has a good effect on improving the performance of intrusion detection systems in an IoT-Based SG.
Rachidi zhour et al. [16]	Hybrid algorithm that combines the Random Forest, DT and Multilayer Perceptron algorithms.	DDoS-HOIC attack, DoS-Slow Loris attacks, FTP-Brute Force, DoS-SlowHTTPTest attacks, DDoS-LOIC-HTTP attacks, SSH-Brute Force, DoS-Hulk attacks, DoS-GoldenEye attacks, Bot, Infiltration, DDoS-LOIC-UDP attack, Brute Force-Web, Brute Force-XSS, SQL Injection.	The hybrid algorithm demonstrated high performance, surpassing Naive Bayes and Multilayer Perceptron (MLP) algorithms. It achieved high accuracy, high true positive rate and the lowest false negative rate for the NSL KDD, UNSW-NB15 and CIC-IDS-2017 datasets.
Avula Venkata Srinadh Reddy et al. [17]	DT using genetic algorithm.	Probe attack and DoS attack.	The tree managing method is the most ideal for the working of the IDS access street and is executed in the hereditary calculation of avoidance.
Muhammad Refansa Akbar et al. [18]	Binary Decision Tree.	-	The proposed system effectively determines the intrusions on Unmanned Aerial Vehicles (UAVs) with average accuracy and precision of 91.6%.
Answer Shees et al. [27]	DT	FDI attack.	The Extra Trees, Random Forest and XGBoost models demonstrated superior performance compared to those reported in the existing literature.
MD Jainul Abudin et al. [28]	Hybrid DT	FDI attack.	The decision tree combined with logistic regression significantly enhanced the performance.

In summary, this proposed work makes the following significant contributions to the field of smart PV systems:

(1) The introduction of a novel ConvXGBoost method for the smart PV inverter system that can not only detect but also identify the location of the attack.
(2) The proposed model is extensively evaluated along with the traditional CNN and DT models on DoS and FDI attack data to prove the effectiveness of combining the models to enhance prediction accuracy.
(3) Furthermore, the developed models are evaluated to effectively see how fast the models were able to detect and identify the location of the attacks.

These contributions pave the way for future research in developing AI models that combine the capabilities of different models to enhance the ability to detect, identify and mitigate more efficiently.

This paper is organized as follows: Section 2 discusses the problem statement that explains the motivation to develop the proposed model to detect and identify cyberattacks in solar PV systems. Section 3 presents the mathematical modeling of cyberattacks. In Section 4, the proposed model is presented with the necessary mathematical equations.

Section 5 presents the existing methods developed for comparison, and Section 6 presents the implementation of the models. Section 7 presents the results of the proposed model in comparison with the developed existing models, and finally, Section 8 presents conclusions.

2. Problem Statement

Over the recent past, electric grids have become increasingly smart with the advent of the latest digital technologies and advanced communication protocols, thereby improving the efficiency and performance of all four facets of electric power systems, namely generation, transmission, distribution and consumption of electricity. This functionality is facilitated by the interconnection of IoT devices, allowing for seamless communications and data exchange between different parts of the system. One of the important challenges with smart grids is the effective and efficient transmission of bulk data without any altercations [29]. 5G communication offers the fastest communication with the least latency, among the available networks. These features may address the challenges of smart grids [30]. Integrating the Advanced Metering Infrastructure (AMI) and Distributed Energy Resources (DERs) with the Internet and providing 5G technology communications (referred to as IoT with 5G) may offer a stable and secure smart grid [31]. Even though the cost of infrastructure and operational costs are higher for 5G communications, the advantages of increased network capacity, low latency and faster data transmission can offset the higher costs [32].

Nevertheless, with the integration of IoT devices and the advent of the 5G network, the smart PV inverter system is still prone to cyber-intrusions due to the vulnerabilities of the integrated system. As seen in the smart PV inverter system of Figure 1, the attacker can interfere with the control signals sent from SCADA and interrupt the operation of the respective controllers. The attacker can jam these control signals, thereby inducing a delay in the system. These delays cause disruptions in the system depending on its withstanding capabilities. Moreover, the attacker can induce false data into these signals that can manipulate the system parameters leading to operation failures due to the disruptions in the normal operation. To evidently show the impact of these cyber-intrusions, a smart solar PV system is developed in the MATLAB/Simulink environment, and the attacks are implemented.

The developed system is a grid-connected 140 kW smart solar PV system that operates irrespective of grid connection or disconnection mode as shown in Figure 1. The major electric circuits in this proposed system are the PV generation system, battery system and inverter control system. The PV system is coupled to a boost converter with control circuitry for operating PV at the maximum power point (MPP). The battery is connected to a buck-boost converter which is controlled by the proportional integral (PI)-based battery control circuitry which helps to maintain the DC bus voltage V_{BUS} at the reference voltage V_{ref_DC} of 400 V.

The inverter system consists of a six-pulse three-bridge inverter with control circuitry designed based on the synchronous generator (SG) dynamic operating characteristics as shown in Figure 2. This Virtual SG (VSG)-based control circuitry will help to operate the inverter control system similar to the traditional SG, thereby maintaining the system inertia. The control circuitry of the proposed VSG-inverter system can be represented using the following equations:

$$P_m = P_{ref} + k_1\left(f_{ref} - f\right) \quad (1)$$

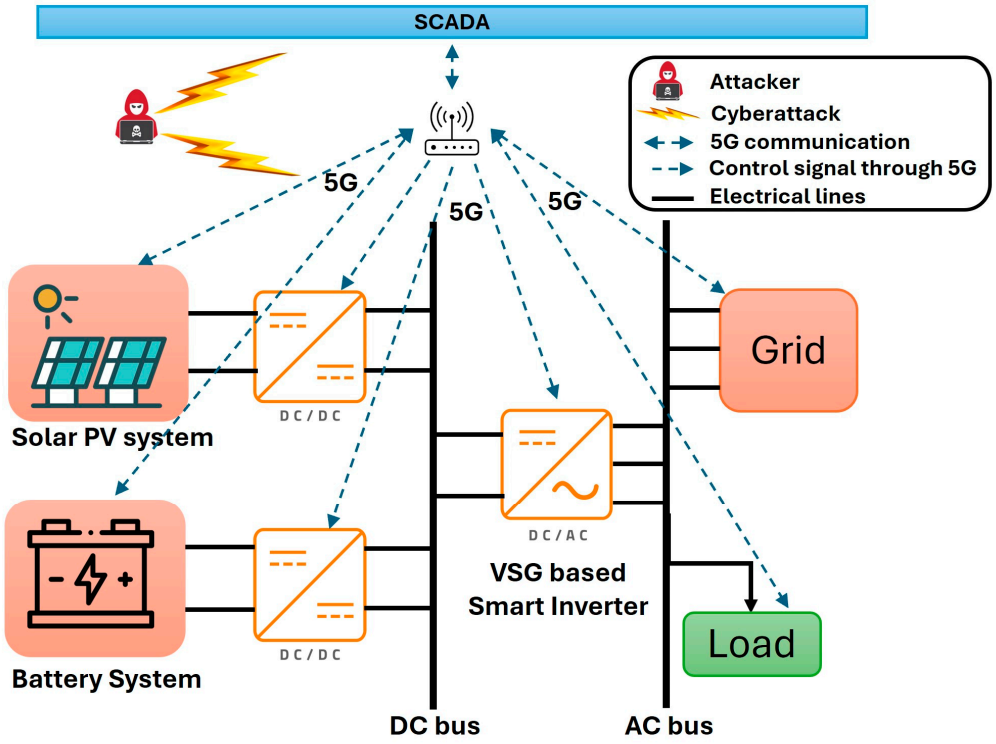


Figure 1. Smart PV inverter system connected to the grid.

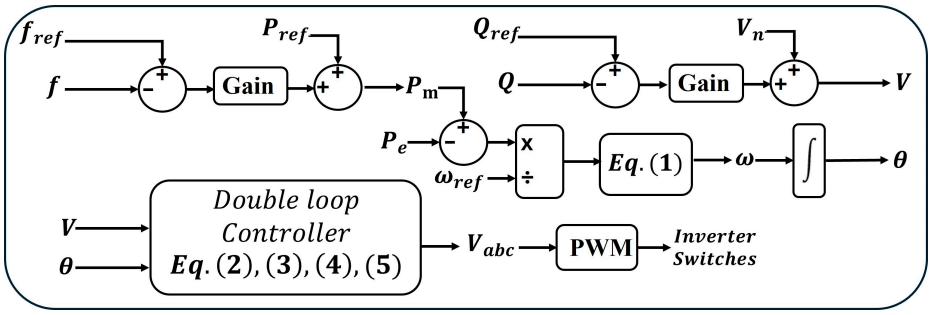


Figure 2. Inverter system control circuitry.

Equation (1) represents the $f - p$ control loop, where P_m is the calculated mechanical power, P_{ref} is the reference active power, f_{ref} is the reference frequency, f is the measured frequency, and k_1 is the gain value.

$$V = V_{ref} + k_2\left(Q_{ref} - Q\right) \tag{2}$$

Equation (2) represents the $Q - V$ control loop, where V is the calculated voltage, Q_{ref} is the reference reactive power, V_{ref} is the reference voltage, Q is the measured reactive power, and k_2 is the gain value.

$$\frac{P_m}{\dot{\theta}_{ref}} - \frac{P_e}{\dot{\theta}_{ref}} = J\ddot{\theta} + D(\dot{\theta} - \dot{\theta}_{ref}) \tag{3}$$

Equation (3) represents the rotor function loop, where θ is the reference angle, J is the virtual inertia, and D is the damping coefficient. This control loop is designed based on the rotor dynamics of the SG, i.e., based on the swing equation.

Further, double loop control circuitry is implemented to generate the reference signals for the Pulse Width Modulation (PWM) generator to control the switches of the inverter. The mathematical modeling of this control loop can be represented as

$$V_d^f = V_d^* + (i_d - i_{sd}^*)\left(k_{p1} + \frac{k_{i1}}{s}\right) - \omega L i_{sq}^* \tag{4}$$

$$V_q^f = V_q^* + \left(i_q - i_{sq}^*\right)\left(k_{p2} + \frac{k_{i2}}{s}\right) + \omega L i_{sd}^* \tag{5}$$

$$i_d = i_d^* + \left(V_d^{ref} - V_d^*\right)\left(k_{p3} + \frac{k_{i3}}{s}\right) - \omega C V_q^* \tag{6}$$

$$i_q = i_q^* + \left(V_q^{ref} - V_q^*\right)\left(k_{p4} + \frac{k_{i4}}{s}\right) + \omega C V_d^* \tag{7}$$

where V_d^f & V_q^f are the final reference signal sent to the PWM generator. V_d^*, V_q^*, i_d^*, i_q^* are the measured voltages and currents after the filter inductor L, and i_{sd}^*, i_{sq}^* are the measured currents after the filter capacitor C. V_d^{ref}, V_q^{ref} are the reference signals generated based on the rotor dynamics. k_{p1}, k_{p2}, k_{p3}, k_{p4} are the respective proportional gains, and k_{i1}, k_{i2}, k_{i3}, k_{i4} are the respective integral gains.

Under normal operation, the smart PV inverter feeds the load with the power produced from the solar PV panels and, if required, from the BES depending on the load requirement and to maintain stability as shown in Figure 3.

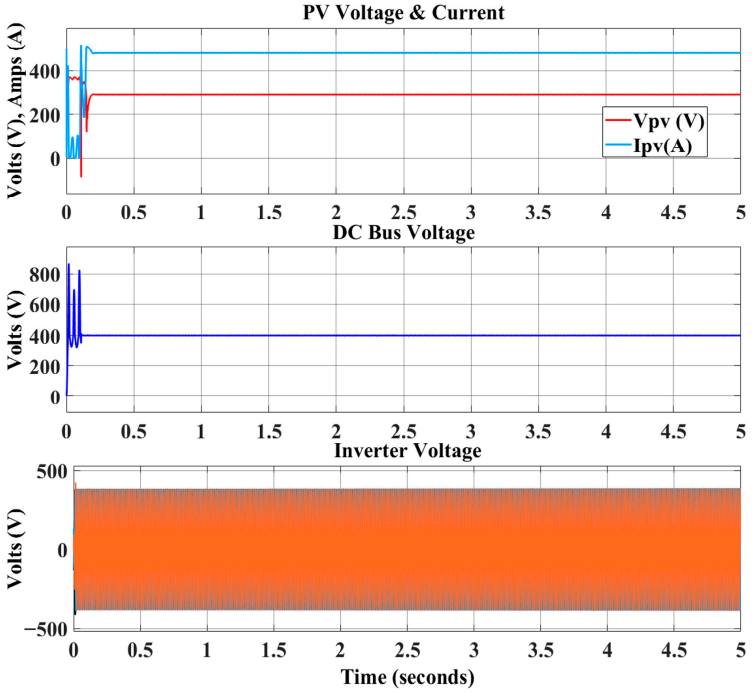


Figure 3. System under normal operating conditions.

Under these operating conditions, the control signals from the SCADA to the respective controllers are reached without any time delay. In this system, it is assumed that the attacker launched a DoS attack on the control signals for a duration of 1 s at time step 2 s as shown in Figure 4a. The intensity of the attack influences the extent of the time delay (elaborated in Section 3), and the disruption of the system is dependent on its ability to withstand the delay. As shown in Figure 4a, when the attack is introduced on the system, it is clearly seen how the DoS attack was able to disrupt the entire system and cause a catastrophic disaster.

In Figure 4b, the FDI attack on the V_{ref} set point of the inverter also shows how this attack can manipulate the system parameters that lead to the disrupted behavior.

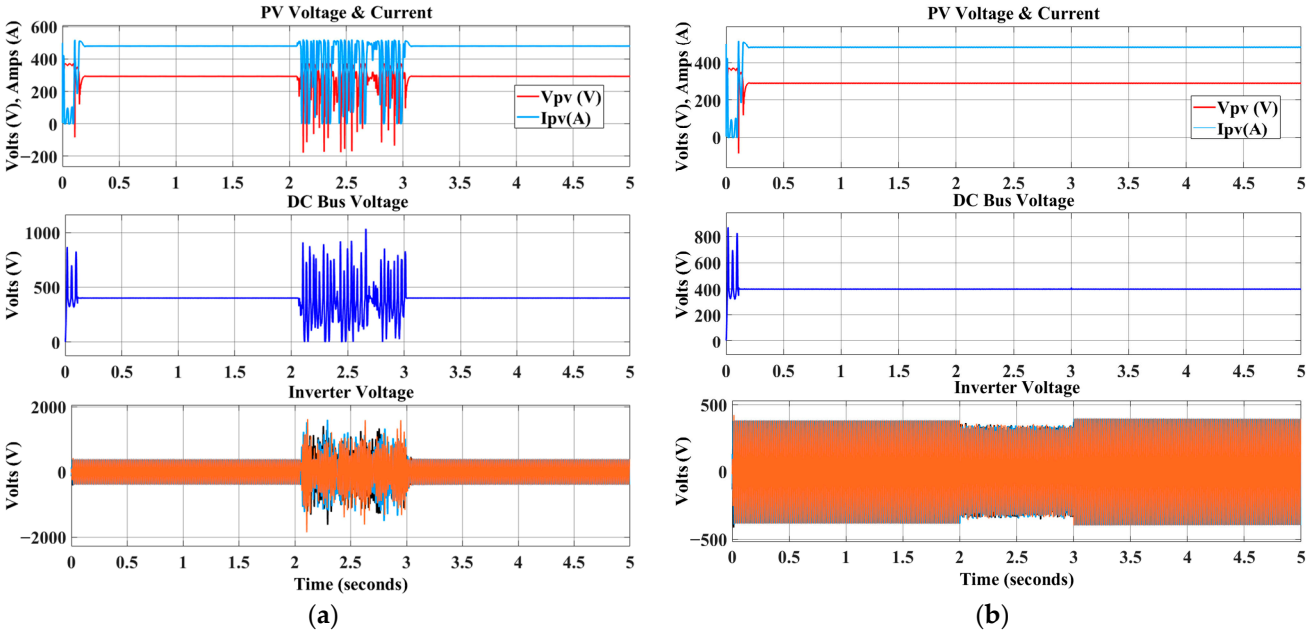


Figure 4. System under (**a**) DoS attack and (**b**) FDI attack on V_{ref}.

These results show why there is a need for effective detection of cyber-intrusions and the mitigation of these intrusions to maintain the system's stability. There is a need for identification of the location of these attacks for effectively mitigating either by isolating the affected system or by providing a means to generate the lost control signal. All these facts serve as a strong motivation for the proposed research.

3. Mathematical Modeling of Attacks

The smart PV system is continuously monitored and controlled by SCADA through the 5G communication lines.

3.1. DoS/DDoS Attack Modeling

The DoS/DDoS attack on this 5G network can be considered in a way that, when this attack happens on the smart PV system, there will be a loss of signal sent from SCADA to the controllers in the smart PV system. This introduces a delay in the control signal, and the duration of the delay depends on the total number of samples lost during the attack. Let $\{x_i\}_{i=0}^{N}$ be the control signal sent from SCADA at time i, N be the total number of samples and N_o be the total number of samples lost during the DoS/DDoS attack on the 5G network, then the original and delayed control signal can be represented as

$$x_{original}(t) = x(t) = \{x_i\}_{i=0}^{N} \tag{8}$$

$$x_{delay}(t) = x(t - N_0) = \{x_i\}_{i=-N_0}^{N-N_0} \tag{9}$$

In other words, this can be interpreted as

$$x_{delay}(t + N_0) = x_{original}(t) \tag{10}$$

where, to get the same sample from the original control signal $x_{original}$, we should add N_0 sample time to the current timestep of x_{delay}.

The attack sequence can be explained as follows: (a) First, the smart PV system operates normally by communicating with the SCADA system through 5G communication lines as shown in Equation (11a). (b) Then, the attacker launches the DoS/DDoS attack on the system starting at sample time of $t_1 \geq 0$ lasting up to t_2, where $t_2 = t_1 + N_0 \leq N$, N_0 is the variable delay that depends on the severity of the attack. During this period, the signal samples are completely lost as shown in Equation (11b). (c) After the attack is cleared, the signal retains the $t_1 + 1$ signal sample as in the post-attack period, as shown in Equation (11c), since the DoS/DDoS attack does not alter the signal integrity. Based on this attack sequence, the composite control signal reaches the smart PV system, and x_{PV} can be expressed as

$$x_{PV}(t) = \begin{cases} x_{original}(t) & if\ 0 \leq t < t_1, pre\ attack \quad (11a) \\ 0 & if\ t_1 < t \leq t_2\ , attack \quad (11b) \\ x_{delay}(t) & if\ t_2 < t \leq N,\ post\ attack \quad (11c) \end{cases}$$

3.2. FDI Attack Modeling

In an FDI attack, the attacker can induce false data into the system that can manipulate the system operations. The attacker can solely control the duration of the attack and the distribution of the false data as long as the attack is detected and mitigated. For the smart PV system, the attacker can change the reference points of the respective controllers. For instance, in the case of the inverter, the FDI attack is implemented on the reference values V_{ref}, P_{ref} and Q_{ref} as shown in Equations (12)–(14), where the function G represents the Gaussian distribution of the false data induced with mean η and variance σ.

$$\hat{V}_{ref_{\text{attack}}} = \mathrm{V}_{ref} + \Delta \mathrm{V}_{ref}; \Delta \mathrm{V}_{ref} \sim \mathrm{G}(\eta, \sigma) \quad (12)$$

$$\hat{P}_{ref_{\text{attack}}} = P_{ref} + \Delta P_{ref}; \Delta P_{ref} \sim \mathrm{G}(\eta, \sigma) \quad (13)$$

$$\hat{Q}_{ref_{\text{attack}}} = Q_{ref} + \Delta Q_{ref}; \Delta Q_{ref} \sim \mathrm{G}(\eta, \sigma) \quad (14)$$

4. Proposed ConvXGBoost Method

ConvXGBoost is a deep learning model that combines the performance of CNN and XGBoost models for better prediction of classes [25]. The ConvXGBoost uses the automatic feature learning capability of the CNN model and the better class prediction capability of the XGBoost. In this section, the mathematical modeling and the architecture of the proposed model are presented.

4.1. Mathematical Representation

In the proposed model, the feature map layer of the traditional CNN model is extracted and given as input to the XGBoost model. From the understanding of the mathematical representation of the CNN presented in [25], the mathematical explanation behind the 1D-CNN architecture proposed for this model can be derived as

For the input data, I, of size $1 \times \mathrm{H}$,

$$I = \{x(p) | 1 \leq p \leq H\} \quad (15)$$

where I is the input data of size 1×18, a 1D array with 18 different parameters of the smart PV system that includes {inverter voltage (d, q-axis), inverter current (d, q-axis), PV voltage, PV current, irradiance, temperature, battery voltage, battery current, DC bus voltage, DC bus current, measured frequency, reference frequency, measured active power, reference active power, measured reactive power, reference reactive power}, and $x(p)$ is the value of

the parameter at the given index p of the input data. The h_k filters or kernels k produce a feature map y from the given input I by sliding the filter k through the input by a stride S_k and with zero padding values. Then, the discrete convolution is represented as

$$\left(I \bigotimes k\right)_v = \sum_{u=-h_k}^{h_k} K_u I_{v+u} \tag{16}$$

In each of the convolution layers, indexed by l, a convolution operation and an additive bias will be applied to the input for the feature mapping indexed by $f \in \{1, 2, ..f(l)\}$. Thus, the output, $y_i^{(l)}$, of the l^{th} layer of the i^{th} feature map can be derived from the output of the previous layer, $y_i^{(l-1)}$, by

$$y_i^{(l)} = \varnothing\left(B_i^{(l)} + \sum_{j=1}^{f(l-1)} K_j^{(l)} * y_j^{(l-1)}\right) \tag{17}$$

where $\varnothing$ is the Rectified Linear Unit (ReLU) activation function, $B_i^{(l)}$ is the bias added at the l^{th} layer, and $K_j^{(l)}$ is the filter. Therefore, the elements of the output of the layer, l, for the feature map, i, $y_i^{(l)}$ at position p can be given as

$$\begin{aligned}\left(y_i^{(l)}\right)_p &= \varnothing\left(\left(B_i^{(l)}\right)_p + \sum_{j=1}^{f(l-1)}\left(K_j^{(l)} \otimes y_j^{(l-1)}\right)_p\right) \\ &= \varnothing\left(\left(B_i^{(l)}\right)_p + \sum_{j=1}^{f(l-1)} \sum_{u=-h_k^l}^{h_k^l} \left(k_j^{(l)}\right)_p \left(y_j^{(l-1)}\right)_{v+u}\right)\end{aligned} \tag{18}$$

A max-pooling layer that further modifies the output by replacing the output with the maximum value within a rectangular neighborhood is used. Let M(.) be the pooling function that is applied on the $y_j^{(l)}$ by passing it through a pooling process of stride S_M and a pooling window of size h_M; then, the output of the max-pooling function will be

$$M\left(y_i^{(l)}\right)_p = max\left(y_i^{(l)}\right)_p \tag{19}$$

where the *max* function is applied to the max-pooling window of the given size. In general, the pooling operation is performed by placing windows of the given size at non-overlapping positions in each feature map and keeping the maximum value per window, thereby subsampling the feature maps. The output from this pooling layer is stretched to a single-column vector and given as an input to the XGBoost model.

The XGBoost of [23] is a powerful end-to-end tree boosting algorithm developed for regression and classification problems based on gradient boosting. In general, a tree ensemble uses K additive functions of classification and regression trees (CARTs) to predict the output Y, for the given input, X.

$$\hat{Y}_i = \sum_{j=1}^{K} f_j(X_i), \quad f_j \in G \tag{20}$$

where X_i represents the training set from the CNN, and the Y_i is the class label of the respective input. f_j is the leaf score of the j^{th} tree, and G represents the set of all K scores

of all the CARTs. The main objective is to learn the j trees by minimizing the following regularized objective function:

$$\begin{aligned} &L(\varphi) = \sum_i l\left(Y_i, \hat{Y}_i\right) + \sum_j \Omega\left(f_j\right) \\ &where,\ \Omega(f) = \gamma T + \tfrac{1}{2}\lambda||\omega||^2 \end{aligned} \tag{21}$$

Here, l is the differentiable convex loss function, which measures the difference between the target label Y_i and the predicted class label $\hat{Y}_i$. The second term, Ω, avoids overfitting by penalizing the complexity of the model. γ, λ are the hyperparameters that control the regularization degree, T is the number of leaves in the tree, and ω is the weight of each leaf. Gradient boosting is effective in regression and classification. XGBoost uses the loss function and implements second-order Taylor expansion, eliminating the constant terms to optimize the objective function. For the i^{th} instance and i^{th} iteration, the simplified objective function can be given as

$$L^{(t)} \simeq \sum_{i=1}^{n} \left[l\left(Y_i, \hat{Y}_i\right) + g_i f_t(X_i) + \frac{1}{2} h_i f_t^2(X_i) \right] + \Omega(f) \tag{22}$$

where $g_i = \partial l\left(Y_i^{(t-1)}, Y_i\right) / \partial \hat{Y}_i^{(t-1)}$ represents the first-order and $h_i = \partial^2 l\left(Y_i^{(t-1)}, Y_i\right) / \partial \left(\hat{Y}_i^{(t-1)}\right)^2$ represents the second-order gradient statistics on the loss function. The constant term $l\left(Y_i, \hat{Y}_i\right)$ can be removed to further simplify the equation as

$$L^{(t)} \simeq \sum_{i=1}^{n} \left[g_i f_t(X_i) + \frac{1}{2} h_i f_t^2(X_i) \right] + \Omega(f) \tag{23}$$

For a fixed tree structure $q(X)$, the optimal weight ω_j^* of each leaf j where $I_j = \{i | q(X_i) = j\}$, representing the instance set of leaf j, can be computed as

$$\omega_j^* = -\textstyle\sum_{i \in I_j} g_i / \sum_{i \in I_j} h_i + \lambda' \tag{24}$$

And the corresponding optimal value can be calculated by

$$\tilde{L}^{(t)} = -\frac{1}{2} \sum_{j=1}^{T} \frac{\left(\sum_{i \in I_j} g_i\right)^2}{\sum_{i \in I_j} h_i + \lambda} + \gamma T \tag{25}$$

The above equation is used as a scoring function to evaluate the quality of the tree structure. But, in practice, an iterative greedy algorithm that starts from a single leaf and progressively appends branches to the tree is used. I_L, I_R are the instance sets of left and right nodes after the split. By letting $I = I_L \cup I_R$, the loss reduction after the split is

$$L_{split} = -\frac{1}{2} \left[\frac{\left(\sum_{i \in I_L} g_i\right)^2}{\sum_{i \in I_L} h_i + \lambda} + \frac{\left(\sum_{i \in I_R} g_i\right)^2}{\sum_{i \in I_R} h_i + \lambda} - \frac{\left(\sum_{i \in I} g_i\right)^2}{\sum_{i \in I} h_i + \lambda} \right] - \gamma \tag{26}$$

4.2. Model Architecture

The proposed model architecture is shown in Figure 5. The model has five phases: (1) dataset collection phase, (2) data preprocessing phase, (3) convolution layer phase, (4) XGBoost phase and (5) testing phase. The process in each phase is described below:

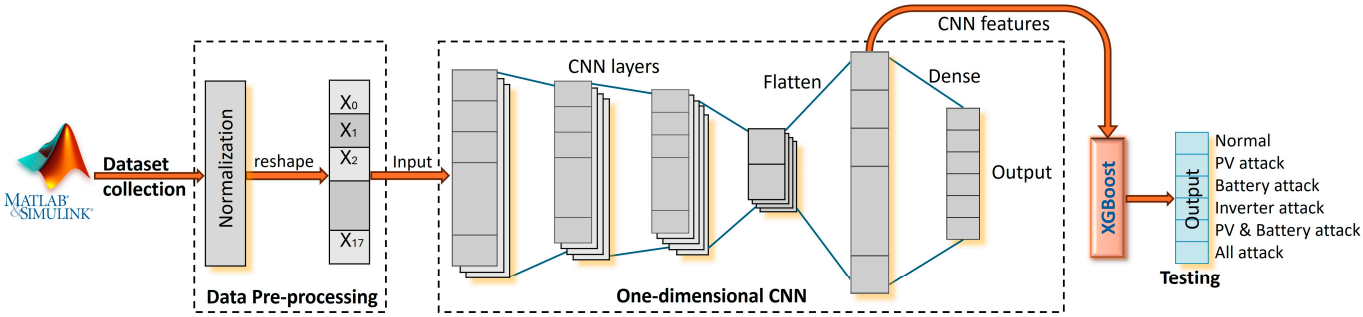


Figure 5. Proposed model architecture.

4.2.1. Dataset Collection Phase

The smart PV system, as shown in Figure 1, is first modeled, and the DoS and FDI attacks are simulated on the developed model for different attack scenarios. The DoS attack is implemented on the communication line that sends the control signal to respective controllers to maintain stable operation, and the FDI attack is implemented on the reference set points of the respective controllers. In total, 650,000 datapoints for each of the DoS attack and the FDI attack were collected by simulating the attacks on different components, out of which, 150,000 datapoints are during normal operation, 100,000 datapoints are for each of the attacks on the PV (Pvattack), battery (Battattack), inverter (Invattack), PV and battery (PVBattattack) and all the components (Allattack). Each time, the model is simulated for 5 s, and the attack is created for a period of 1 s from time 2 s to 3 s. Moreover, the data are downsampled by a factor of 10 during the collection process. In the same way, to evaluate the scalability of the proposed model, the proposed PV system is further expanded by adding a fuel cell (FC) system onto the DC bus (PV-FC system), as shown in Figure 6. The FC system is coupled with a DC/DC converter with control circuitry that helps to maintain the output voltage of this at the reference bus voltage V_{ref_DC}. It is important to note that the FC system has a capacity of 5 kW and a DC bus voltage of 400 V. Also, the ratings and parameters of the PV system and battery energy storage system are the same as the system in Figure 1. Along with the 18 different parameters of the smart PV system as mentioned in Section 4.1, three more parameters, reference FC power, FC voltage and FC current, were collected by simulating a DoS and FDI attack. In total, 650,000 datapoints were collected for each of the DoS and FDI attacks on the PV (Pvattack), battery (Battattack), FC (FCattack), inverter (Invattack) and all components (Allattack).

4.2.2. Data Preprocessing Phase

In this phase, the data collected are first normalized between [−1,1]. Normalization of data is a crucial step in the implementation of ML models. Different features have different scales, without normalization, the features with higher scales may dominate the lower-scale features, thereby avoiding biased learning. Once the data are normalized, they are then reshaped into a 1D vector for feeding into the CNN model. The data are split into 70% for training and 30% for evaluating the model.

4.2.3. Convolution Layer Phase

In this phase, a CNN model is trained by reshaped training data for automatic feature extraction. Once trained, the featuring mapping layer of the CNN is used as an input to the XGBoost model. The sequence of CNN layers is as follows: Conv1D (32,3), Conv1D (32,3), Max Pooling (2), Dropout 0.2, Conv1D (64,3), Conv1D (64,3), Max Pooling (2), Dropout 0.3, Conv1D (128,3), Conv1D (128,3), Max Pooling (2), Dropout 0.4, Flatten, Dense, Output layer (SoftMax).

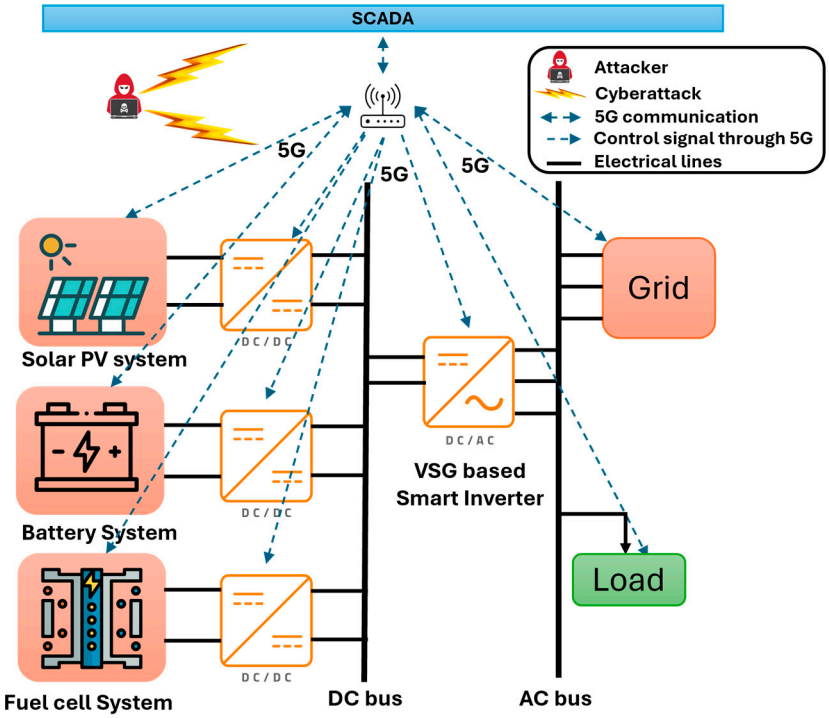


Figure 6. Smart PV inverter along with a fuel cell system connected to the grid.

The activation function is "ReLU", and hyperparameters are set to the following values: batch size = 64, optimizer = RMSprop, learning rate = 0.001, decay rate = 1×10^{-6} and epochs = 150.

4.2.4. XGBoost Phase

In this phase, the features extracted from the CNN model are used as input to the XGBoost model to train it for predicting the class labels. The hyperparameters of the XGBoost are set to the following values: estimators = 300, learning rate = 0.1 and max depth = 10.

4.2.5. Testing Phase

Once the model is trained with the training dataset, the model is then evaluated on the test dataset on the following parameters: precision, sensitivity, specificity, accuracy and F1-score, as described below:

- Precision: This evaluation metric measures the accuracy of positive predictions made by the model. It can be calculated by

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \tag{27}$$

- Here, True Positives (TP) are the cases where the model predicts a positive outcome for the positive class, and False Positives (FP) are the cases where the model predicts a positive outcome for a negative class.
- Sensitivity/Recall: It is the measure of the actual positive proportion predicted by the model. This metric shows the sensitivity of the model and can be calculated by

$$Sensitivity = TP/(TP + False\ Negatives) \tag{28}$$

- Here, False Negatives (FN) are the cases where the model predicts a negative outcome for a positive class.

- Specificity: This metric measures the accuracy of the negative predictions made by the model. This metric shows how specific the model is in identifying the negative outcomes and can be calculated by

$$Specificity = \frac{True\ Negatives}{True\ Negatives + FP} \tag{29}$$

- Here, True Negatives (TN) are the cases where the model predicts a negative outcome for a negative class.
- Accuracy: Accuracy measures the total correctness of the model, and this can be calculated by

$$Accuracy = \frac{TP + TN}{Total\ Predictions} \tag{30}$$

- F1-Score: This particular metric provides the harmonic mean of precision and sensitivity/recall. It is particularly useful in case of class imbalances and can be calculated by

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{31}$$

- To aggregate the calculated performance metrics for all the classes, two methods, macro-average and micro-average, are used. In the macro-average, the performance metrics of each class are computed and averaged across all the classes. For instance, in the macro-average, the precision for N classes can be computed as

$$Precision_{Macro} = \frac{1}{N}\sum_{i=1}^{N} Precision_i \tag{32}$$

- In the micro-average, the contributions of all the classes are aggregated before computing the respective performance metric. Computation of precision using the micro-average for N classes can be performed as

$$Precision_{Micro} = \frac{TP_1 + TP_2 + \ldots + TP_N}{TP_1 + FP_1 + TP_2 + FP_2 + \ldots + TP_N + FP_N} \tag{33}$$

Moreover, the proposed model and the other developed models are further evaluated on the proposed smart PV system by introducing the attacks at different timesteps and by evaluating how fast the models are able to detect and identify the attack for effective mitigation.

5. Existing Methods

The proposed model is compared with two state-of-the-art studies to show the effectiveness of the performance in detecting and identifying the components of the solar PV system under the DoS and FDI attacks. The selected state-of-the-art models are implemented and tested using the same dataset. The proposed model is a combination of the capabilities of CNN and DT models. So, for the comparative study, the state-of-the-art CNN model and the DT model are selected to analyze the performances of the models.

5.1. CNN Model

The structure of the CNN model [8,9,12–14] selected for comparative study is similar to that of the one developed for the proposed model. Moreover, the hyperparameters are also the same for both models. In short, the same CNN model used for the feature extraction in the proposed methodology is used for the comparative study, as the objective of the proposed methodology is to show the effectiveness when the models are combined.

5.2. DT Model

The DT model was proposed by researchers in detecting cyber-intrusions [15–18]. All the hyperparameters for this model are set to default values and trained using the training dataset. In general, the default values allow the DT to grow until it perfectly fits the training dataset.

6. Implementation of the Proposed Conventional Methods Through Simulation Platforms

In this work, all the training and testing were conducted using Python 3.11.7 in the Jupyter Notebook (version 6.5.4) under the open-source Anaconda Navigator (version 2.5.2) and by using MATLAB R2024a on 11th Gen Intel® Core™ i7-11700K CPU @ 3.60 GHz, Memory: 32.0 GiB, GPU: NVIDIA GeForce RTX 3060 Ti 8 GiB OS: Windows 11Pro.

The proposed methodology is implemented in two different environments, as shown in Figure 7. The proposed systems, as shown in Figures 1 and 6, are modeled in the MATLAB/Simulink environment to generate the required data for training the ML models. The details are collected over normal operations and during the attack at multiple locations as described in the previous section. Moreover, the collected data are pre-processed and then exported to the Python environment where the proposed ConvXGBoost method and the conventional CNN and DT models are structured and trained. These models are trained in the Python environment and then evaluated on the test dataset by generating the confusion matrix and by the performance metrics such as precision, sensitivity, specificity, accuracy and F1-score. The confusion matrix and the respective results are demonstrated in the next section.

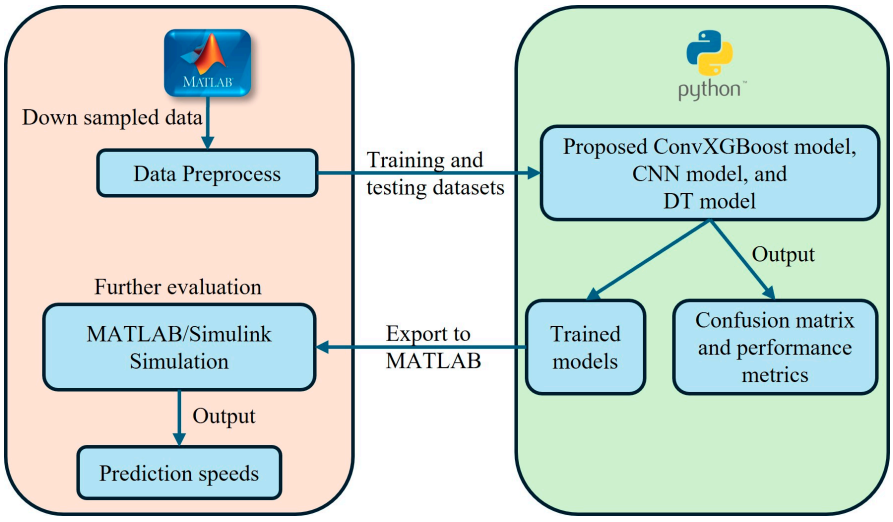


Figure 7. Flow of proposed research in multiple environments.

Furthermore, the trained ML models, i.e., the proposed ConvXGBoost model, conventional CNN and DT models are imported into the MATLAB/Simulink environment for further evaluation of their performance in the aspect of how fast the models can detect and identify the attack in the simulation environment.

7. Results and Discussion

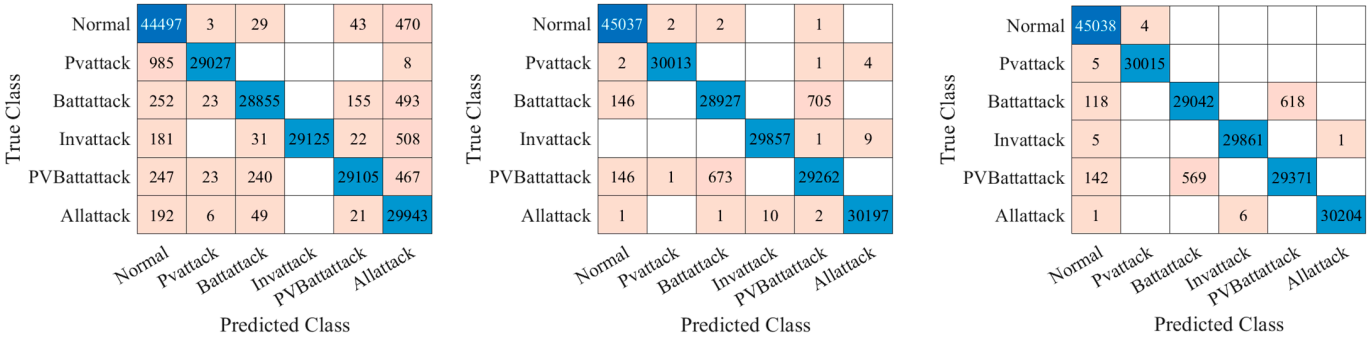
As discussed earlier in Sections 4 and 6, the proposed model, along with the comparative models, is evaluated extensively on two different systems, a smart PV system and smart PV-FC system, under two different attack scenarios in each system. The results are provided below.

7.1. Proposed Smart PV System

Section 7.1 provides the results and discussion on the performance of the proposed models along with the conventional CNN and DT models during the DoS attack and FDI attack on the proposed smart PV system.

7.1.1. Analysis of the Confusion Matrix and Performance Metrics for Smart PV System

Figure 8 shows the confusion matrix of the proposed model and the comparative models during the DoS attack. The confusion matrix presents how the model performed on each of the classes and how well the model can predict the classes. It is evident from the confusion matrix that the proposed model was able to detect and identify the DoS attack with fewer misclassifications than the CNN and DT models.



(**a**) Conventional CNN model (**b**) Conventional DT model (**c**) Proposped ConvXGBoost model

Figure 8. Confusion matrix of proposed and conventional methods during DoS attack on proposed smart PV system.

Figure 8a presents the confusion matrix of the CNN model. The CNN model was able to predict most of the classes perfectly, but there was a significant amount of datapoints that were misclassified by the model. In particular, the model predicted most of the attack datapoints as normal and as Allattack. Moreover, it misclassified a significant number of datapoints as an attack on different components. Based on these values from the confusion matrix, the performance metrics are calculated and presented in Table 3. From Table 3, it is seen that the accuracy of the model is 97.72%, whereas the macro-average of precision is found to be 97.95%, sensitivity/recall is 97.63%, specificity is 99.53%, and F1-score is 97.76%.

Figure 8b presents the confusion matrix of the DT model. It is observed that the DT model performed better than the CNN model with few misclassified datapoints. The accuracy of this model is calculated to be 99.12% as shown in Table 3. Macro-average values of precision, sensitivity/recall, specificity and F1-score are found to be 99.10%, 99.05%, 99.82% and 99.08%, respectively.

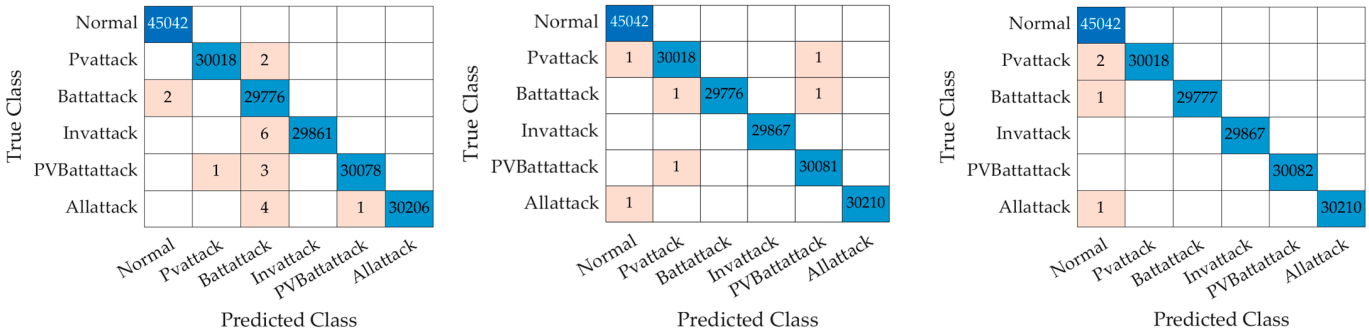
The confusion matrix of the proposed ConvXGBoost model is presented in Figure 8c. From this confusion matrix, it is seen that the proposed method can classify almost every datapoint perfectly, and there are only a few misclassified datapoints compared to the other two models. The performance accuracy of this proposed model is found to be 99.25%. From Table 3, the macro-average of the performance metrics is seen as precision—99.23%, sensitivity/recall—99.18%, specificity—99.85% and the F1-score—99.21%.

Figure 9 shows the confusion matrix of the proposed model and the comparative models during the FDI attack, and Table 4 presents the respective performance metrics during this attack. It is observed that the FDI attack on the system was relatively easy to detect and identify. However, it is evident from these results that the proposed model was able to detect and identify the FDI attack almost perfectly, whereas the CNN and DT models had notable misclassifications when compared with the proposed model.

Table 3. Performance metrics of proposed ConvXGBoost model along with CNN and DT models during DoS attack on proposed smart PV system.

Performance Metrics	Classes						Macro-Average	Micro-Average
	Normal	PV Attack	Battery Attack	Inverter Attack	PV and Battery Attack	All Attack		
CNN								
Precision	0.9599	0.9981	0.988	1	0.9918	0.939	0.9795	0.9772
Sensitivity/Recall	0.9879	0.9669	0.969	0.9752	0.9675	0.9911	0.9763	0.9772
Specificity	0.9876	0.9997	0.9979	1	0.9985	0.9982	0.9953	0.9954
Accuracy	0.9772	0.9772	0.9772	0.9772	0.9772	0.9772	0.9772	0.9772
F1-Score	0.9737	0.9823	0.9784	0.9874	0.9795	0.9643	0.9776	0.9772
DT								
Precision	0.9935	0.9999	0.9772	0.9997	0.9763	0.9996	0.9910	0.9912
Sensitivity/Recall	0.9999	0.9998	0.9714	0.9997	0.9727	0.9995	0.9905	0.9912
Specificity	0.9980	1	0.9959	0.9999	0.9957	0.9999	0.9982	0.9982
Accuracy	0.9912	0.9912	0.9912	0.9912	0.9912	0.9912	0.9912	0.9912
F1-Score	0.9967	0.9998	0.9743	0.9997	0.9745	0.9996	0.9908	0.9912
ConvXGBoost								
Precision	0.9940	0.9999	0.9808	0.9998	0.9794	0.9998	0.9923	0.9925
Sensitivity/Recall	0.9999	0.9998	0.9756	0.9998	0.9764	1	0.9918	0.9925
Specificity	0.9982	1	0.9966	1	0.9963	1	0.9985	0.9985
Accuracy	0.9925	0.9925	0.9925	0.9925	0.9925	0.9925	0.9925	0.9925
F1-Score	0.9970	0.9999	0.978	0.9998	0.9779	0.9999	0.9921	0.9925

Figure 9a presents the confusion matrix of the CNN model. The CNN model was able to predict most of the classes perfectly, but there were a few datapoints that were misclassified by the model. In particular, the model predicted most of the attack datapoints as Battattack. Based on these values from the confusion matrix, the performance metrics are calculated and presented in Table 4. From Table 4, it is seen that the accuracy of the model is 99.99%. Moreover, the macro-average of precision and sensitivity/recall is 99.99%, specificity is 100%, and F1-score is 99.99%.



(**a**) Conventional CNN model (**b**) Conventional DT model (**c**) Proposped ConvXGBoost model

Figure 9. Confusion matrix of proposed and conventional methods during FDI attack on proposed smart PV system.

Figure 9b presents the confusion matrix of the DT model. It is observed that the DT model performed perfectly with few misclassified datapoints. The accuracy of this model is calculated to be 100% as shown in Table 4. For Battattack, the values of precision, sensitivity/recall and F1-score are all found to be 99.9%. The macro-averages of all the other metrics are calculated to be 100%.

Table 4. Performance metrics of proposed ConvXGBoost model along with CNN and DT models during FDI attack on proposed smart PV system.

Performance Metrics	Classes						Macro-Average	Micro-Average
	Normal	PV Attack	Battery Attack	Inverter Attack	PV and Battery Attack	All Attack		
CNN								
Precision	1	1	0.9995	1	1	1	0.9999	0.9999
Sensitivity/Recall	1	0.9999	0.9999	0.9998	0.9999	0.9998	0.9999	0.9999
Specificity	1	1	0.9999	1	1	1	1	1
Accuracy	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
F1-Score	1	1	0.9997	0.9999	0.9999	0.9999	0.9999	0.9999
DT								
Precision	1	0.9999	1	1	0.9999	1	1	1
Sensitivity/Recall	1	0.9999	0.9999	1	1	1	1	1
Specificity	1	1	1	1	1	1	1	1
Accuracy	1	1	1	1	1	1	1	1
F1-Score	1	0.9999	1	1	1	1	1	1
ConvXGBoost								
Precision	0.9999	1	1	1	1	1	1	1
Sensitivity/Recall	1	0.9999	1	1	1	1	1	1
Specificity	1	1	1	1	1	1	1	1
Accuracy	1	1	1	1	1	1	1	1
F1-Score	1	1	1	1	1	1	1	1

The confusion matrix of the proposed ConvXGBoost model is presented in Figure 9c. From this confusion matrix, it is seen that the proposed method can classify almost every datapoint perfectly. The performance accuracy of this proposed model is found to be 100%. From Table 4, the macro-averages of the performance metrics precision, sensitivity/recall, specificity and the F1-score are all 100%.

These performance metrics under both the DoS and FDI attack scenarios clearly indicate that the proposed model outperformed both the CNN and DT models during the FDI attack. The proposed model integrates the strengths of these two models, resulting in improved performance over state-of-the-art models in both attack detection and component identification of the proposed system.

7.1.2. Additional Evaluation in Terms of Operational Speeds for Smart PV System

Since the models are tested on the simulation environment and evaluated on how fast they can predict the attack, a window length of 5 ms is used to predict the final output. The performance of these models is presented in Table 5, showing the time taken for each model to detect and identify the cyberattack and presenting the instances where the models misclassified certain attacks. As seen from Table 5, the ConvXGBoost model was able to detect and identify the attacks better and quicker than the CNN and DT models. Though in some instances, the CNN was able to detect and identify the attack a bit quicker than the proposed model, it misclassified the attack location for certain instances. Due to these factors, though the CNN model was able to detect the attack ~10 ms faster than the proposed ConvXGBoost method in some instances, overall, the proposed method proved to be more efficient in detecting and identifying the location of the cyber-intrusions.

Table 5. Performance of proposed ConvXGBoost model along with CNN and DT models in terms of operational speeds during DoS attack on proposed smart PV system.

		Pvattack	**Battattack**	**Invattack**	**PVBattattack**	**Allattack**
True Class	**Pvattack**	**DT** (57.7 ms), **CNN** (54.4 ms) **ConvXGBoost** (54.17 ms)				
	Battattack		**DT** (129.07 ms), **CNN** (121.7 ms) **ConvXGBoost** (122.4 ms)		**DT**, **CNN**, **ConvXGBoost** (misclassified)	
	Invattack			**DT** (104.34 ms), **CNN** (60.1 ms) **ConvXGBoost** (70.35 ms)		
	PVBattattack	**DT, CNN, ConvXGBoost** (misclassified)	**CNN**, **ConvXGBoost** (misclassified)		**DT** (305.7 ms), **CNN** (305.3 ms) **ConvXGBoost** (360.62 ms)	**DT** (misclassified)
	Allattack	**DT**, **CNN**, **ConvXGBoost** (misclassified)	**DT**, **CNN** (misclassified)	**DT**, **CNN**, **ConvXGBoost** (misclassified)	**DT**, **CNN** (misclassified)	**DT** (305.7 ms), **CNN** (305.3 ms) **ConvXGBoost** (360.62 ms)
				Predicted Class		

Under the FDI attack, all the models performed extremely well in terms of operational speed. The proposed model, along with the conventional CNN and DT models, was able to detect and identify the FDI attacks on different components of the proposed system immediately with a window length of 5 ms.

These metrics evidently prove the efficacy and effectiveness of the proposed ConvXGBoost methodology that can enhance the performance by combining the capabilities of the CNN and XGBoost in not just detecting but also identifying cyber-intrusions in a smart solar PV inverter.

7.2. Smart PV-FC System (With FC Connected to the DC Bus)

Section 7.2 provides the results and discussion on the performance of the proposed models along with the conventional CNN and DT models during the DoS attack and FDI attack on the smart PV-FC system, as shown in Figure 6.

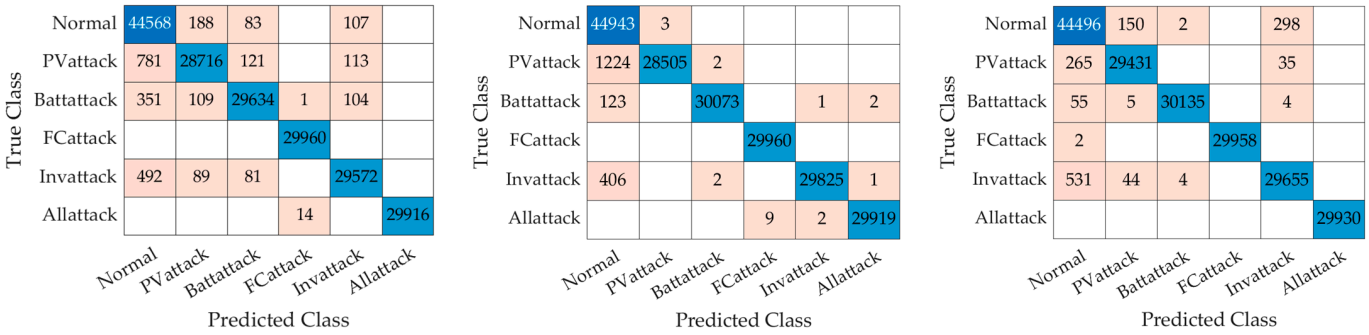
7.2.1. Analysis of the Confusion Matrix and Performance Metrics for Smart PV-FC System

The confusion matrix of the proposed model and the comparative models during the DoS attack are presented in Figure 10.

Figure 10a presents the confusion matrix of the CNN model. The CNN model was able to predict most of the classes perfectly, but there was a significant amount of datapoints that were misclassified by the model. In particular, the model predicted most of the attack datapoints as Pvattack and Battattack. From these confusion matrices, the performance metrics are calculated and presented in Table 6. From Table 6, the accuracy of the CNN model is calculated to be 98.65%, whereas the macro-averages of precision, sensitivity/recall and F1-score are found to be 98.85%, and specificity is 99.73%.

Figure 10b presents the confusion matrix of the DT model. From this, it is clearly observed that the DT model performed better than the CNN model with most of its misclassified datapoints as Pvattack. The accuracy of this DT model for a DoS attack

is calculated to be 99.09%, as shown in Table 6. The macro-average values of precision, sensitivity/recall and F1-score are found to be 99.09%, and specificity is 99.82%.



(**a**) Conventional CNN model (**b**) Conventional DT model (**c**) Proposped ConvXGBoost model

Figure 10. Confusion matrix of proposed and conventional methods during DoS attack on smart PV-FC system.

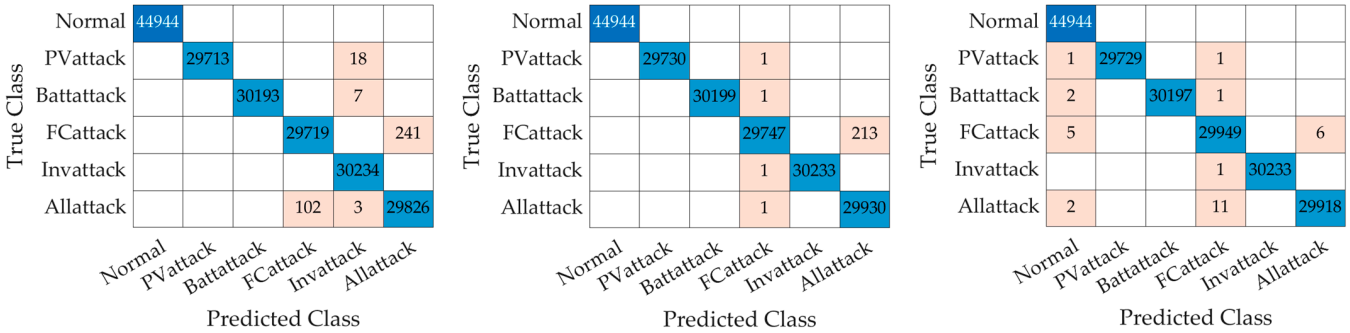
The confusion matrix for the proposed ConvXGBoost model is shown in Figure 10c. This matrix indicates that the proposed method is able to classify nearly all datapoints accurately, with only a few misclassifications compared to the other two models. The performance accuracy of this proposed model is found to be 99.28%. From Table 6, the macro-average of the performance metrics is seen as precision—99.28%, sensitivity/recall—99.28%, specificity—99.86% and the F1-score—99.28%. These performance metrics clearly indicate that the proposed model outperformed both the CNN and DT models under the DoS attack.

Table 6. Performance metrics of the proposed ConvXGBoost model along with CNN and DT models during DoS attack on smart PV-FC system.

Performance Metrics	Classes						Macro-Average	Micro-Average
	Normal	PV Attack	Battery Attack	Inverter Attack	PV and Battery Attack	All Attack		
CNN								
Precision	0.9648	0.9867	0.9905	0.9995	0.9892	1	0.9885	0.9865
Sensitivity/Recall	0.9916	0.9659	0.9813	1	0.9781	0.9995	0.9861	0.9865
Specificity	0.9892	0.9977	0.9983	0.9999	0.9980	1	0.9972	0.9973
Accuracy	0.9865	0.9865	0.9865	0.9865	0.9865	0.9865	0.9865	0.9865
F1-Score	0.9780	0.9762	0.9859	0.9997	0.9836	0.9998	0.9872	0.9865
DT								
Precision	0.9625	0.9999	0.9999	0.9997	0.9999	0.9999	0.9936	0.9909
Sensitivity/Recall	0.9999	0.9588	0.9958	1	0.9865	0.9996	0.9901	0.9909
Specificity	0.9883	1	1	0.9999	1	1	0.9980	0.9982
Accuracy	0.9909	0.9909	0.9909	0.9909	0.9909	0.9909	0.9909	0.9909
F1-Score	0.9808	0.9789	0.9978	0.9998	0.9931	0.9998	0.9917	0.9909
ConvXGBoost								
Precision	0.9812	0.9933	0.9998	1	0.9888	1	0.9938	0.9928
Sensitivity/Recall	0.9900	0.9899	0.9979	0.9999	0.9808	1	0.9931	0.9928
Specificity	0.9943	0.9988	1	1	0.9980	1	0.9985	0.9986
Accuracy	0.9928	0.9928	0.9928	0.9928	0.9928	0.9928	0.9928	0.9928
F1-Score	0.9856	0.9916	0.9988	1	0.9848	1	0.9935	0.9928

Figure 11 shows the confusion matrix of the proposed model and the comparative models during the FDI attack, and Table 7 presents the respective performance metrics during this attack. Similar to the other system, it is observed that the FDI attack on

the system was relatively easy to detect and identify. However, the proposed model outperforms the CNN and DT models and is able to detect and identify FDI attacks perfectly. Meanwhile, the CNN and DT models have notable misclassifications when compared with the proposed model.



(**a**) Conventional CNN model (**b**) Conventional DT model (**c**) Proposped ConvXGBoost model

Figure 11. Confusion matrix of proposed and conventional methods during FDI attack on smart PV-FC system.

Table 7. Performance metrics of proposed ConvXGBoost model along with CNN and DT models during FDI attack on smart PV-FC system.

Performance Metrics	Classes						Macro-Average	Micro-Average
	Normal	PV Attack	Battery Attack	Inverter Attack	PV and Battery Attack	All Attack		
CNN								
Precision	1	1	1	0.9966	0.9991	0.9920	0.9979	0.9981
Sensitivity/Recall	1	0.9994	0.9998	0.9920	1	0.9965	0.9979	0.9981
Specificity	1	1	1	0.9994	0.9998	0.9985	0.9996	0.9996
Accuracy	0.9981	0.9981	0.9981	0.9981	0.9981	0.9981	0.9981	0.9981
F1-Score	1	0.9997	0.9999	0.9943	0.9995	0.9942	0.9979	0.9981
DT								
Precision	1	1	1	0.9999	1	0.9929	0.9988	0.9989
Sensitivity/Recall	1	1	1	0.9929	1	1	0.9988	0.9989
Specificity	1	1	1	1	1	0.9987	0.9998	0.9998
Accuracy	0.9989	0.9989	0.9989	0.9989	0.9989	0.9989	0.9989	0.9989
F1-Score	1	1	1	0.9964	1	0.9964	0.9988	0.9989
ConvXGBoost								
Precision	0.9998	1	1	0.9995	1	0.9998	0.9999	0.9998
Sensitivity/Recall	1	0.9999	0.9999	0.9996	1	0.9996	0.9998	0.9998
Specificity	0.9999	1	1	0.9999	1	1	1	1
Accuracy	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998
F1-Score	0.9999	1	1	0.9996	1	0.9997	0.9998	0.9998

Figure 11a presents the confusion matrix of the CNN model. The CNN model was able to predict most of the classes perfectly, but there were a few datapoints that were misclassified by the model. In particular, the model predicted some of the FCattack datapoints as Allattack. Based on these values from the confusion matrix, the performance metrics are calculated and presented in Table 7. From Table 7, the accuracy of the CNN model is calculated to be 99.81%.

Figure 11b presents the confusion matrix of the DT model. In the case of the DT model, it is observed that the DT model performed perfectly with a few of the FCattack datapoints misclassified as Allattack datapoints. The accuracy of this model for the FDI attack is calculated to be 99.89%, as shown in Table 7.

The confusion matrix of the proposed ConvXGBoost model is presented in Figure 11c. From this confusion matrix, it is seen that the proposed method can classify almost every datapoint perfectly. The performance accuracy of this proposed model is found to be 99.98%. Though the FDI attack is relatively easy to detect and identify, the performance metrics clearly indicate that the proposed model outperformed both the CNN and DT models.

The proposed model combines the capabilities of these two models and thereby performs better than the state-of-the-art models in not only detecting the attack but also in identifying the components under attack of the proposed system.

7.2.2. Additional Evaluation in Terms of Operational Speeds for Smart PV-FC System

The performance of the proposed ConvXGBoost model along with the CNN and DT models during the DoS attack and FDI attack on the smart PV-FC system are presented in Table 8. This table shows the time taken for each model to detect and identify the cyberattack and also presents the instances where the models misclassified certain attacks. During the DoS attack, it is evident from this table that the ConvXGBoost model was able to detect and identify the attacks better and quicker than the CNN and DT models. Moreover, the DT misclassified the Pvattack as Battattack and the Invattack as Allattack. Though the CNN was able to detect and identify the attack, the proposed model is quicker, especially during the PV attack where the CNN model takes about 69.5 ms while the proposed ConvXGBoost model only takes 5 ms.

During the FDI attack on the system, all the models performed very well and were able to detect and identify the attacks almost immediately, except for the FCattack where the DT model took around 5.6 ms and the CNN took around 36.63 ms to detect and identify the attack. Also, for the Allattack, the CNN and the proposed model took 29.24 ms.

Overall, these metrics evidently prove the efficacy and effectiveness of the proposed ConvXGBoost methodology that can enhance the performance by combining the capabilities of the CNN and the XGBoost in not just detecting but also identifying the cyber-intrusions in a smart solar PV-FC inverter system.

Table 8. Performance of proposed ConvXGBoost model along with CNN and DT models in terms of operational speeds during DoS attack and FDI attack on smart PV-FC system.

		Pvattack	**Battattack**	**FCattack**	**Invattack**	**Allattack**
True Class	**Pvattack**	**DT** (FDI: 5 ms) **CNN** (DoS: 69.5 ms, FDI: 5 ms) **ConvXGBoost** (DoS: 5 ms, FDI: 5 ms)	**DT** (DoS: misclassified)			
	Battattack		**DT** (DoS: 5 ms, FDI: 5 ms), **CNN** (DoS: 5 ms, FDI: 5 ms) **ConvXGBoost** (DoS: 5 ms, FDI: 5 ms)			
	FCattack		**CNN** (DoS: misclassified)	**DT** (DoS: 5 ms, FDI: 5.6 ms), **CNN** (FDI: 36.63 ms) **ConvXGBoost** (DoS: 5 ms, FDI: 5 ms)		
	Invattack				**DT** (FDI: 5 ms) **CNN** (DoS: 5 ms, FDI: 5 ms) **ConvXGBoost** (DoS: 5 ms, FDI: 5 ms)	**DT** (DoS: misclassified)
	Allattack					**DT** (DoS: 5 ms, FDI: 5 ms), **CNN** (DoS: 5 ms, FDI: 29.24 ms) **ConvXGBoost** (DoS: 5 ms, FDI: 29.24 ms)
				Predicted Class		

8. Conclusions and Future Work

In this work, a novel ConvXGBoost method that combines the feature extraction capabilities of the CNN and the robust classification feature of the XGBoost method for the detection and identification of cyberattacks on a smart solar PV inverter system is proposed. The conclusions that can be drawn from this work are as follows:

(1) The performance metrics presented show how well the proposed method was able to detect and identify the attacks and how it can improve the predictions of the conventional CNN models by combining them with the XGBoost model.
(2) The proposed model has an accuracy of 99.25% when compared with the 97.72% of the traditional CNN and 99.12% of traditional DT models during the DoS attack on a smart PV system and an accuracy of 99.28% when compared to the 98.65% of the traditional CNN and 99.09% of the traditional DT during the DoS attack on a smart PV-FC system to prove its supremacy.
(3) The proposed model along with the other comparative models, when tested under the FDI attack on a smart PV system, was found to have an accuracy of almost 100%, and for the smart PV-FC system, the accuracy for the proposed model was 99.98% while the traditional CNN model had 99.81%, and the traditional DT model had 99.89%.
(4) Moreover, further evaluation of these models on how fast they are able to detect the attack and identify the location of the attack in the smart PV and smart PV-FC inverter systems demonstrates that the proposed model is able to detect and identify the attack faster than the other models.

The future work of this research can go into several directions. There is a growing need for a detection and identification mechanism with the emerging smart grids. The future work will be focused on the development of advanced techniques for the mitigation of cyber-intrusion. The proposed model helps to detect and identify the component that is comprised that can help in the effective mitigation of the cyber-intrusion by correcting the affected signals of the respective controller using advanced control techniques or by removing the affected component to minimize the effect on the connected system.

The proposed model should be further validated using real-time data, and its efficacy in addressing uncertainties should be optimized for enhanced performance. The smart PV inverter system experimental testbed will be developed in the future for the generation of data and to test the proposed strategy by inducing cyber-intrusions. The computational costs in the implementation of this proposed work along with the hardware requirement for the experimental testbed will be explored.

Detailed analysis of 5G communications for the smart PV inverters needs to be explored. 5G-enabled IoT devices have been explored that will be integrated with the smart PV system experimental testbed for evaluating the real-time attack scenarios on these networks for effective data generation.

Through ongoing research and enhancements in the aforementioned areas, the proposed ConvXGBoost method can present a robust solution for addressing the cybersecurity challenges faced by smart PV systems.

Author Contributions: Conceptualization, S.N.V. and M.H.A.; methodology, S.N.V. and M.H.A.; software, S.N.V.; validation, S.N.V. and M.H.A.; resources, S.N.V. and M.H.A.; writing—original draft preparation, S.N.V.; writing—review and editing, S.N.V. and M.H.A.; supervision, M.H.A.; project administration, M.H.A.; funding acquisition, M.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors gratefully acknowledge the partial financial support from the Electrical and Computer Engineering Department of The University of Memphis to complete this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Solar Integration: Inverters and Grid Services Basics | Department of Energy. Available online: https://www.energy.gov/eere/solar/solar-integration-inverters-and-grid-services-basics (accessed on 16 May 2024).
2. Tao, J.; Umair, M.; Ali, M.; Zhou, J. The Impact of Internet of Things Supported by Emerging 5G in Power Systems: A Review. *CSEE J. Power Energy Syst.* **2020**, *6*, 344–352. [CrossRef]
3. Wang, C. State Prediction for Smart Grids under DoS Attack Using State Correlations under Optimized PMU Deployment. In Proceedings of the 2022 5th International Symposium on Autonomous Systems (ISAS), Hangzhou, China, 8–10 April 2022. [CrossRef]
4. Zhong, Y.; Wang, Z.; Li, J.; Fan, Z.; Ji, L.; Chen, K. A Review of Features, Vulnerabilities, Cyber-Attacks and Protective Actions in Smart Grid Systems. In Proceedings of the 2023 IEEE 6th International Electrical and Energy Conference, CIEEC 2023, Hefei, China, 12–14 May 2023; pp. 171–176. [CrossRef]
5. Tuyen, N.D.; Quan, N.S.; Linh, V.B.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. [CrossRef]
6. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6225. [CrossRef] [PubMed]
7. Boyaci, O.; Rasoul Narimani, M.; Davis, K.; Serpedin, E. Cyberattack Detection in Large-Scale Smart Grids Using Chebyshev Graph Convolutional Networks. In Proceedings of the 2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022, Alanya, Turkey, 29–31 March 2022; pp. 217–221. [CrossRef]
8. Ho, S.; Al Jufout, S.; Dajani, K.; Mozumdar, M. A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network. *IEEE Open J. Comput. Soc.* **2021**, *2*, 14–25. [CrossRef]
9. Di Lu, K.; Zhou, L.; Wu, Z.G. Representation-Learning-Based CNN for Intelligent Attack Localization and Recovery of Cyber-Physical Power Systems. *IEEE Trans. Neural Netw. Learn. Syst.* **2023**, *35*, 6145–6155. [CrossRef]
10. Abdelkhalek, M.; Ravikumar, G.; Govindarasu, M. ML-Based Anomaly Detection System for Der Communication in Smart Grid. In Proceedings of the 2022 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2022, New Orleans, LA, USA, 24–28 April 2022. [CrossRef]
11. Bitirgen, K.; Filik, Ü.B. A Hybrid Deep Learning Model for Discrimination of Physical Disturbance and Cyber-Attack Detection in Smart Grid. *Int. J. Crit. Infrastruct. Prot.* **2023**, *40*, 100582. [CrossRef]
12. Mao, J.; Zhang, M.; Xu, Q. CNN and LSTM Based Data-Driven Cyberattack Detection for Grid-Connected PV Inverter. In Proceedings of the IEEE International Conference on Control and Automation, ICCA 2022, Naples, Italy, 27–30 June 2022; pp. 704–709. [CrossRef]
13. Alabsi, B.A.; Anbar, M.; Rihan, S.D.A. CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks. *Sensors* **2023**, *23*, 6507. [CrossRef] [PubMed]
14. Zhang, G.; Li, J.; Bamisile, O.; Xing, Y.; Cao, D.; Huang, Q. Identification and Classification for Multiple Cyber Attacks in Power Grids Based on the Deep Capsule CNN. *Eng. Appl. Artif. Intell.* **2023**, *126*, 106771. [CrossRef]
15. Taghavinejad, S.M.; Taghavinejad, M.; Shahmiri, L.; Zavvar, M.; Zavvar, M.H. Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree. In Proceedings of the 2020 6th International Conference on Web Research, ICWR 2020, Tehran, Iran, 22–23 April 2020; pp. 152–156. [CrossRef]
16. Zhour, R.; Khalid, C.; Abdellatif, K. Hybrid Intrusion Detection System Based on Random Forest, Decision Tree and Multilayer Perceptron (MLP) Algorithms. In Proceedings of the 10th International Conference on Wireless Networks and Mobile Communications, WINCOM 2023, Istanbul, Turkiye, 26–28 October 2023. [CrossRef]
17. Reddy, A.V.S.; Reddy, B.P.; Sujihelen, L.; Mary, A.V.A.; Jesudoss, A.; Jeyanthi, P. Intrusion Detection System in Network Using Decision Tree. In Proceedings of the International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2022, Erode, India, 23–25 March 2022; pp. 1186–1190. [CrossRef]
18. Akbar, M.R.; Nuha, H.H.; Mugitama, S.A. Intrusion Detection on Unmanned Aerial Vehicle (UAV) Using Binary Decision Tree. In Proceedings of the International Conference on ICT Convergence 2023, Melaka, Malaysia, 23–24 August 2023; pp. 633–638. [CrossRef]
19. Omitaomu, O.A.; Niu, H. Artificial Intelligence Techniques in Smart Grid: A Survey. *Smart Cities* **2021**, *4*, 548–568. [CrossRef]
20. Jiao, J. Application and Prospect of Artificial Intelligence in Smart Grid. *IOP Conf. Ser. Earth Environ. Sci.* **2020**, *510*, 022012. [CrossRef]

21. Zhang, Q.; Yang, Y.; Ma, H.; Wu, Y.N. Interpreting CNNs via Decision Trees. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 6254–6263. [CrossRef]
22. Lan, T.; Hu, H.; Jiang, C.; Yang, G.; Zhao, Z. A Comparative Study of Decision Tree, Random Forest, and Convolutional Neural Network for Spread-F Identification. *Adv. Space Res.* **2020**, *65*, 2052–2061. [CrossRef]
23. Chen, T.; Guestrin, C. XGBoost: A Scalable Tree Boosting System. In Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, 13–17 August 2016; pp. 785–794. [CrossRef]
24. Abdulrahman Lateef, R.; Rodhan Abbas, A. A Proposed ConvXGBoost Model for Human Activity Recognition with Multi Optimizers. *Webology* **2022**, *19*, 1703–1715. [CrossRef]
25. Thongsuwan, S.; Jaiyen, S.; Padcharoen, A.; Agarwal, P. ConvXGB: A New Deep Learning Model for Classification Problems Based on CNN and XGBoost. *Nucl. Eng. Technol.* **2021**, *53*, 522–531. [CrossRef]
26. Understanding Denial-of-Service Attacks | CISA. Available online: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks (accessed on 19 May 2024).
27. Shees, A.; Tariq, M.; Sarwat, A.I. Cybersecurity in Smart Grids: Detecting False Data Injection Attacks Utilizing Supervised Machine Learning Techniques. *Energies* **2024**, *17*, 5870. [CrossRef]
28. Abudin, M.J.; Thokchom, S.; Naayagi, R.T.; Panda, G. Detecting False Data Injection Attacks Using Machine Learning-Based Approaches for Smart Grid Networks. *Appl. Sci.* **2024**, *14*, 4764. [CrossRef]
29. Jichkar, R.; Paraskar, S.; Parteki, R.; Ghosh, M.; Deotale, T.; Pathan, A.S.; Bawankar, S.; Thakare, L.P. 5g: An Emerging Technology and Its Advancement. In Proceedings of the International Conference on Emerging Trends in Engineering and Technology, ICETET 2023, Nagpur, India, 28–29 April 2023. [CrossRef]
30. Chahar, S.; Kaur, K. Internet of Things with 5G Technology: A Critical Review. In Proceedings of the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023, Greater Noida, India, 12–13 May 2023; pp. 1402–1406. [CrossRef]
31. Rituraj, R.; Varkonyi, D.T.; Mosavi, A.; Koczy, A.V. 5G for Smart Grids: Review, Taxonomy, Bibliometrics, Applications and Future Trends. In Proceedings of the INES 2023—27th IEEE International Conference on Intelligent Engineering Systems 2023, Nairobi, Kenya, 26–28 July 2023; pp. 275–284. [CrossRef]
32. Gunawan, A.; Gajon Odang, B.G.; Honggiarto, K.; Cahyadi, F.L. Understanding the Uses and Potential of IoT with 5G Technology Compared to 4G LTE: A Systematic Literature Review. In Proceedings of the 2023 International Conference on Information Management and Technology, ICIMTech 2023, Malang, Indonesia, 24–25 August 2023; pp. 101–106. [CrossRef]