*electronics*

*Article*

# Evaluation of Deep Learning Techniques in PV Farm Cyber Attacks Detection

**Ghufran F. Hassan [1,*], Oday A. Ahmed [1] and Muntadher Sallal [2]**

[1] Department of Electrical Engineering, University of Technology, Baghdad 35299, Iraq; oday.a.ahmed@uotechnolgy.edu.iq

[2] Department of Computing and Informatics, Bournemouth University, Bournemouth BH3 7JH, UK; msallal@bournemouth.ac.uk

* Correspondence: eee.21.05@grad.uotechnology.edu.iq

**Abstract:** Integrating intelligent grids with the internet increases the amount of unauthorized input data which directly or indirectly influences electrical system control and decision-making. Photovoltaic (PV) farms that are linked to the power grid are susceptible to cyber attacks which may disrupt energy infrastructure and compromise the security, stability, and resilience of the electrical system. This research proposes a new model for cyber threat detection in PV farm, named as Cyber Detection in PV farm (CDPV), which makes use of deep learning methods based solely on point-of-common coupling (PCC) detectors. In this paper, a thorough cyber attack model for a photovoltaic (PV) farm is developed, where the simulation of four kinds of cyber attacks is provided. Furthermore, this paper evaluates the role of three deep learning techniques including convolutional neural network (CNN), artificial neural network (ANN), and long short-term memory (LSTM), in PV cyber threat detection. The findings demonstrate that, at the DC/DC converter and DC/AC inverter sides, the proposed CDPV model based on deep learning techniques (CNN, ANN, and LSTM) can improve the cyber detection accuracy and resilience under various attack scenarios.

**Keywords:** cyber-attack; photovoltaic farm; machine learning; power electronic converters; cyber-physical system; cyber security

Academic Editor: Domenico Caputo

Received: 6 October 2024
Revised: 26 December 2024
Accepted: 6 January 2025
Published: 29 January 2025

**Citation:** Hassan, G.F.; Ahmed, O.A.; Sallal, M. Evaluation of Deep Learning Techniques in PV Farm Cyber Attacks Detection. *Electronics* **2025**, *14*, 546. https://doi.org/10.3390/electronics14030546

## 1. Introduction

In many nations, strategies addressing climate change must include Renewable Energy Source (RES) technologies, which are also critical to decarburization initiatives. Due to its eco-friendliness, sustainability, and lack of operating costs, solar photovoltaic (PV) is one of the most significant potential distributed energy resources when considering generating variety in the energy industry [1]. Over the past 20 years, there has been a remarkable, huge percentage rise in the nominal capacity of solar photovoltaic systems. Although there are many advantages to PV systems, PV systems' unpredictable behavior makes managing the power system complex [2]. To maintain the stable operation of PV systems generation, the MPPT (Maximum Power Point Tracking) controller is required [3].

The integration of new technical components into an intelligent grid has been achieved through the combination of photovoltaic systems (PVs) and other renewable energy source (RES) technologies to control and manage power flow. These components, collectively referred to as Information and Communication Technologies (ICT), include innovations such as the Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA) systems, among others, which are integral to the operation of the intelligent electrical network [4,5]. However, critical elements of the connected power grid are vulnerable to cyberattacks and other threats. Depending on their severity, such attacks could undermine the monitoring capabilities of the intelligent grid, adversely affecting the security, stability, resilience, and overall reliability of the power system, either in the short term or over an extended period [6].

As previously explained, integrating intelligent grids with the internet increases the influx of unauthorized input data, which directly or indirectly influences the control and decision-making processes of electrical systems. The interaction between cyber networks and power systems has gradually transformed these systems into multifunctional, diverse, and complex cyber-physical power systems (CPPSs) [7]. The technical capabilities of cyber systems in CPPSs play a pivotal role in enhancing the observability and controllability of electrical networks [8]. Given the interdependence of cyber and physical systems, the performance of cyber systems significantly affects the operation of physical power systems. CPPSs encompass all critical areas of energy systems, including electricity generation, transmission, distribution, utilization, and marketing [9]. However, the transfer of information and data over the internet is vulnerable to cyber threats, such as Data Integrity Attacks (DIAs), which aim to modify data unauthorizedly to deceive systems into making erroneous decisions. Extensive research has explored DIAs in legacy electrical infrastructure, including smart grids and DC microgrids. To address these vulnerabilities, both model-based and data-driven techniques have been developed to mitigate the risks [10].

## 2. Problem Statement

Photovoltaic (PV) farms linked to the power grid are susceptible to cyberattacks, which have the potential to disrupt energy infrastructure and compromise the security, stability, and resilience of the electrical system. Therefore, it is essential to evaluate the potential impacts of such attacks on PV farms and develop effective methods for their detection. In previous studies, researchers utilized the Micro Phasor Measurement Unit (μPMU) to gather data aimed at optimizing the attack detection process. By employing low sampling rates from raw electrical waveforms and signals—such as voltage, current, harmonics, and frequency—they extracted valuable information about the stability of electrical grids. These studies utilized μPMU to collect low sampling rates of raw electrical waveform data and improve the detection of assaults on electrical grids. In contrast, we leverage the full range of electrical signal data without relying on μPMU to achieve higher accuracy in detecting and diagnosing attacks. Specifically, this paper evaluates deep learning techniques in cyber security detection within PV farm-based point-of-common coupling (PCC) detectors. Furthermore, there is a lack of accurate data, which involves several attack scenarios on PV farms. Therefore, this paper introduces a PV farm dataset that simulates critical attacks on PV farms. This dataset facilitates the accurate evaluation of deep learning techniques in cyber attack detection in PV farms. Moreover, this paper focuses on detecting Data Integrity Attacks (DIA) in photovoltaic (PV) systems, covering four attack scenarios, two of which are introduced and analyzed for the first time in this study. The following problem is discussed in this paper: how can the deep sequence learning approach identify the cyber threats in PV farms utilizing one phase of the current signal and the voltage signal without using μPMU?

This paper proposes a new model for cyber threat detection in PV farm, named as Cyber Detection in PV farm (CDPV), which makes use of deep learning methods based solely on point-of-common coupling (PCC) detectors. In CDPV, PV systems employ a single voltage sensor and a single current sensor at the PCC to identify and handle many cyber-attacks on the DC/DC and the DC/AC power electronic converting devices. In practical applications, encrypting the communication route may guarantee waveform data security. ANN, CNN, and LSTM are the three data-driven methodologies used as comparative techniques in this research.

## 3. Contributions

The developments and the contributions of our work are

1. Propose a novel PV model designed to simulate four critical cyberattacks that significantly compromise data integrity. Unlike earlier PV models, the proposed structure incorporates individual converter controls for each PV unit and employs an LC inverter filter for enhanced performance and realism.
2. Propose a new model for cyber threat detection in PV farms, named Cyber Detection in PV farm (CDPV). CDPV employs several deep learning methods to detect security issues in PV farms. These methods include CNN, ANN, and LSTM.
3. This paper presents a novel PV farm dataset featuring various attack scenarios aimed at compromising the data integrity of PV systems. The primary objective of creating this dataset is to facilitate the evaluation of deep learning techniques for detecting cyberattacks on PV systems.
4. In-depth evaluation of deep learning techniques in PV cyber attack detection. Specifically, a new evaluation methodology is adopted based on multiclass classification with a high sample rate from the waveform to enhance the attack detection.

## 4. Paper Organization

The paper is organized as follows: Section 5 provides background and related work; Section 6 explores the Proposed Cyber Detection model in PV (CDPV). Section 7 focuses on model evaluation and Implementation. Section 8 presents and discusses the results. Finally, Section 9 presents the conclusions.

## 5. Background and Related Work

### *5.1. Background*

PV panels, DC/DC converters, DC/AC inverters, a controlling device, and an electricity meter make up typical PV farms. The PV array is linked to the network through an on-grid inverter. Many of the PV panels, DC/DC converter, and DC/AC inverter can be connected in parallel to form the PV farm, as shown in Figure 1.

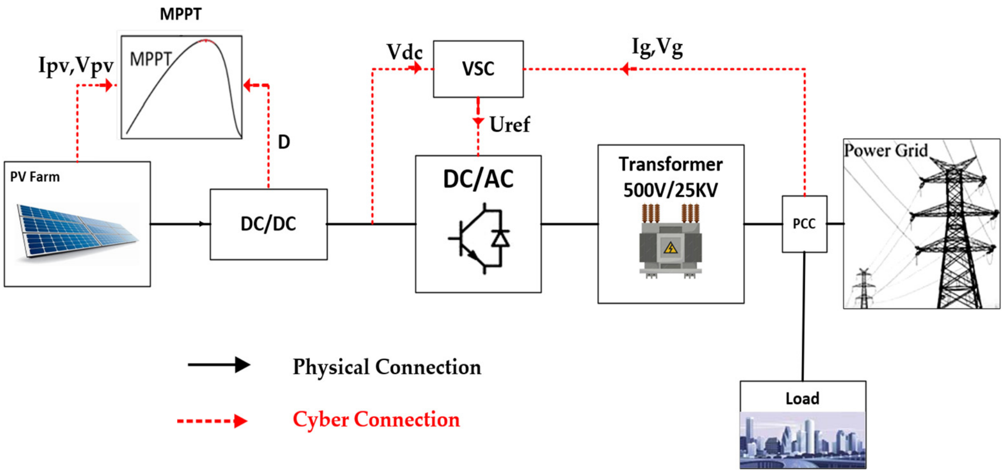


**Figure 1.** PV Farm configuration.

The photovoltaic panel and the DC/AC inverter are connected via a DC/DC converter. To guarantee that the greatest amount of power is taken during varied irradiance and temperature circumstances, the converter performs maximum power point tracking (MPPT) on the comprehensive I/V characteristics of the photovoltaic array. To maximize the power extracted from the PV array, the DC/DC converter is typically constructed as a step-up converter, and the DC/DC controller is MPPT, which applies a perturb and observe (P&O) approach. Throughout this process, the PV array's voltage and power output vary. For each cycle, the tracker measures the voltage and current of the PVs. By analyzing power variations, it calculates the actual solar power generated by the PV system and adjusts the pulse width modulation (PWM) to regulate the switch's input signal. This process is integrated into the Maximum Power Point Tracking (MPPT) mechanism [11]. Advanced converters utilize a variety of MPPT techniques [12].

Energy storage systems (ESSs) and solar energy facilities collaborate to charge batteries during the day and discharge them at night [13]. Control devices collect measurement data from various sensors distributed throughout the photovoltaic (PV) system, including temperature, irradiation, energy, power, voltage, and current data. This data is used to monitor the efficiency of the PV system, enabling the identification of degradation and failures that could impact the system's flexibility and reliability [14]. Multiple sensors continuously assess PV system efficiency and detect potential degradation, such as in the DC-link capacitor, which is critical for minimizing ripple in the output waveforms between DC devices. Filters play a vital role in reducing harmonic distortion between the power grid and the inverter, enhancing system performance. The inverter regulator typically facilitates the transfer of electricity from the DC circuit to the AC network. The PV arrays, inverter, and grid are interconnected through a wireless communication system that gathers operational data. Figure 1 illustrates the cyber-physical connections within the PV farm. The total electricity generated by PV farms is monitored using meters installed for residential and commercial users [15]. Advanced control strategies and integration inverters enable PV farms to provide grid support and meet customer demands as large-scale PV farms become increasingly integrated into the power system. The cyber-physical attacks which occur on PV systems can be classified into four main types [16,17]:

(a) Type One: This category involves direct physical attacks on hardware, such as tampering with wires, inverters, combiner boxes, or PV modules. A notable example includes the widespread removal and theft of photovoltaic panels, which has been among the most prevalent attacks in recent years.

(b) Type Two: This type refers to an attack that targets the inverter itself, the inverter controller, and its algorithms.

(c) Type Three: This type of attack involves injecting false information into the data to deceive operators and manipulate sensor readings, targeting the monitoring and diagnostic systems. The increasing digitalization of solar energy plants and the widespread use of IoT devices for data collection, transmission, and communication within PV systems make such attacks feasible. In response, many inverter manufacturers are strengthening their devices and placing a higher emphasis on cybersecurity.

(d) Type Four: This category encompasses attacks targeting the electrical network, potentially compromising the overall safety and functionality of the plant. Examples include falsifying electricity demand or isolating the PV system from the network. By manipulating voltage levels or triggering breakers, attackers can disconnect PV inverters from the electrical system.

### 5.2. Related Work

This section provides an explanation of the appropriate literature that represents the basis for further investigation of cyber security in PV farms' power electronics. PV farms are subject to cyber-attacks which aim to compromise their sensors, control signals, and data communication capabilities.

Several studies have focused on the vulnerabilities of the control converters which can be utilized by cyber attacks. A survey by [1] highlights the importance of balancing systems performance and cyber-physical interactions to ensure robust and resilient control strategies. Various cases on grid-tied power converters, including DFIG, HVDC, STATCOM, DSTATCOM, and microgrids, are performed in this study. On the other hand, a parallel control framework is proposed in [18], which introduces a model predictive controller (MPC) and a proportional integral controller (PIC), aiming at improving converters' dynamic performances in hydropower plants. Specifically, in the study [19] focuses on enhancing IoT cyber security and improving real-time cyber-attack detection by using sensor data processing techniques that facilitate the exploration of physical layer security, low-complexity encryption, and authentication methods. Similarly, vulnerabilities and cyber threats in PV systems are studied and analyzed in [20]. Precisely, a range of cyber threats in PV, including Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM) attacks, and Data Integrity attacks (DIAs) are discussed and analyzed in this study.

Critical energy infrastructures are becoming more vulnerable as hackers broaden their attack vectors to cover more parts of PV systems and communication networks. Regarding cyber-attack detection approaches, attack detection challenges are analyzed in [21]. Specifically, this study provided an in-depth analysis of the obstacles to the cyber and physical attack detection on the PV systems, in particular, the PV system grid-connected via the HCADI (High-Dimensional Data-Driven Cyber Physical Attack Detection and Identification) technique, which requires a training stage as well as offering significant enhancements. On the other hand, a defensive mechanism for grid-tied photovoltaic (PV) systems is proposed in [22], which is based on dynamic watermarking. Specifically, this research examined the performance of a single-phase inverter using a safeguarding method where data manipulation detection is achieved via signals. Furthermore, the study concluded that this dynamic technique effectively mitigates threats and enhances system stability by analyzing individual events and their impacts. This approach utilizes the DC-link voltage as a constant voltage source while disregarding the effects of the MPPT method.

Machine learning and deep learning techniques have been pivotal in detecting cyber attacks targeting physical infrastructures [23]. Specifically, an analysis of data-driven methods in PV farms such as Decision Trees (DT), Convolutional Neural Networks (CNN), k-Nearest Neighbors (KNN), Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Long Short-Term Memory (LSTM) was presented in [24]. The effectiveness of these techniques, leveraging data from the Micro Phasor Measurement Unit (μPMU), was evaluated for enhancing attack detection. The benefits of data-driven approaches in managing complex power grids were highlighted in [25]. This study addressed device-level security for power electronics converters and proposed a cyber-physical security architecture for a 980 kW PV farm. The PV farm features seven converters connected in parallel to the electrical grid. This architecture offers a chance to examine the impact of cyber attacks on control loops by using reduced PMU data sampling rates to achieve effective detection by comparing two data-driven approaches, LSTM and support vector machine (SVM).

Regarding PV attack detection accuracy when using data-driven methods, authors in [26] introduced a defence strategy which integrates a one-class recognition approach with a breach diagnostic model. Finally, the research in [27] explored machine learning techniques, specifically convolutional neural networks (CNNs), to detect cyberattacks in photovoltaic (PV) farms integrated into a large grid with 37 buses, following the IEEE standard. This approach achieved high detection accuracy and resilience across various attack scenarios. Additionally, a defense strategy was developed using a multi-layer Long Short-Term Memory (LSTM) model to effectively identify the presence of attacks on PV farms.

In Summary, several previous attempts have been made to address the challenges of cyber attacks detection in PV using data-driven models and automated defense methods based on machine learning and deep learning techniques. These attempts show several limitations in detection accuracy, efficiency, and performance. Table 1 presents a compilation of the related works that explore and propose models of cyber attack detection in the context of PV farms.

**Table 1.** The comparison of the previous cyber attack detection techniques.

| Ref. | Method | Strength | Weaknesses |
|---|---|---|---|
| [21] | HCADI | Provide a unique method that combines binary matrix factorization for attack diagnosis with leveraging score-based attack detection. | It does not address the constraints associated with adopting the suggested approach in real time and putting the diagnosis process before detection for enhanced detection attacks. |
| [22] | Dynamic watermarking | Introduce a comprehensive explanation of the defensive mechanism and several possible assault strategies utilizing a 5 kw PV farm. | The defensive system requires validation. |
| [24] | Data driven | Present an analysis of research results that validate the possibility of using µPMU for attack detection in the photovoltaic (PV) farm. | The suggested approach lacks practical application and does not provide analysis details for each attack. |
| [25] | LSTM, SVM | Conduct an analysis of the effects of the DIAs on various control loops within the Photovoltaic (PV) farm. | Detecting attacks is a binary classification issue in that the data is classified into two categories: normal and abnormal. |
| [26] | MLSTM, data driven | The suggested technique has been assessed in a PV smart grid benchmark model using comprehensive quantitative analysis. A applying comparison, the traditional data-driven methodologies have assessed. | A one-class detection approach is used to determine if a photovoltaic (PV) farm is being targeted by an attack. |

**Table 1.** *Cont.*

| Ref. | Method | Strength | Weaknesses |
|---|---|---|---|
| [27] | Machin learning | Provide a comprehensive examination and comparison of several forms of cyber-attacks and physical faults that may occur in photovoltaic (PV) farms. These include attacks on data integrity, replay assaults, open-circuit faults, short-circuit faults, and advanced cyber threats. | Does not explore the mechanism used to prevent oversampling of data and address the suggested strategy's limitations in resolving this problem. |

## 6. The Proposed Detection Model in PV (CDPV)

Due to the limitations of cyber attack detection methods mentioned earlier, this paper presents a new detection model, named as Cyber Detection in PV (CDPV), which assesses and identifies cyberattacks occur in the controllers of PV system converters. In contrast to conventional methods that employ waveform sensors in every PV converter, the CDPV relies on dependable sensing that helps capturing live PV data. CDPV collects data from PV farm sensors to investigate potential attacks on the controllers of PV converters. The second major step that the CDPV achieves is to apply a deep learning detection model on the collected data, aiming to detect cyber attacks with optimal predicted efficiency. The deep learning detection model is in Figure 2.

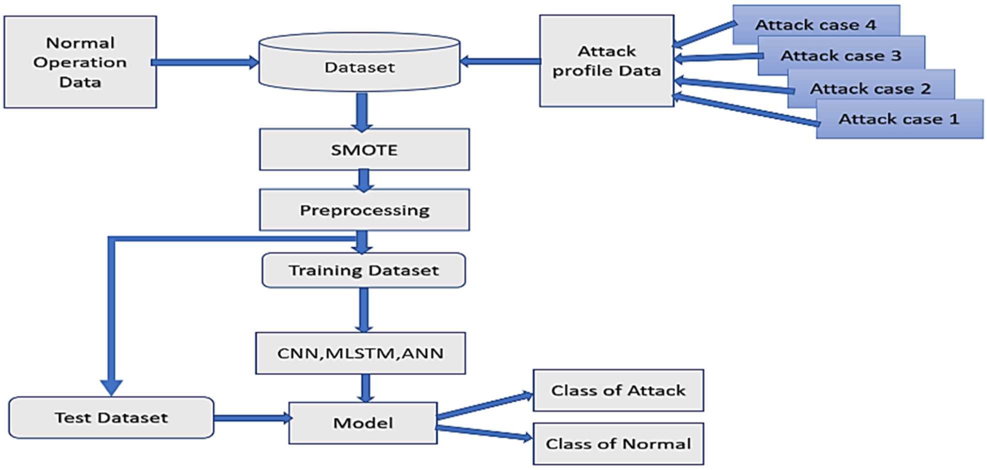


**Figure 2.** Flowchart of the CDPV detection model.

### *Model Overview*

The CDPV model has the following main components, as pictured in Figure 2: Dataset generation, SMOTE, Preprocessing, Training and Testing Dataset, Deep learning (CNN, MLSTM, ANN), and Model (Attack Classification). The details of how these components work is deferred until Section 7.

- Data collection: In this phase, live data is collected from PV sensors, which will be fed into the training and testing model. For the CDPV evaluation purpose, we introduced a dataset generation method involving four PV farm attack cases. More details regarding dataset generation and PV farm modelling are deferred to Section 7.1.
- SMOTE: After generating the dataset, the SMOTE technique is applied. SMOT addresses the class imbalance in the dataset by creating synthetic examples of the minority class (in this case, unusual or attack cases).

- Preprocessing: After making the classes balance in the dataset, data preparation converts unstructured data into a comprehensible format and eliminates unforeseen distortions generated by Simulink simulations to avert inaccuracies in the data sample.
- Training and Testing Dataset: The dataset is divided into training and testing sets. Training data instructs algorithm models by parameter adjustment while testing data assesses model performance and generalization by evaluating its predictive capability on unseen data.
- Deep learning (CNN, MLSTM, ANN): We have used three well-known supervised approaches: ML/DL multiclass classification algorithms, including ANNs, LSTMs, and CNNs. The processing capabilities of each approach vary according to the complexity of the model; by comparing and evaluating them, we can determine which is best.
- Model (Attack Classification): Finally, the trained model is used to classify new data into two categories: usual (non-attack) and unusual (attack). This classification is based on the patterns learned during the training phase. The model's output will indicate whether a particular data point is standard or an attack, helping identify potential threats.

## 7. Model Implementation and Evaluation

### *7.1. Dataset Generation*

In this phase, live data is collected from PV sensors, which will be fed into the training and testing model. For the CDPV evaluation purpose, we introduced a dataset generation method involving four PV farm attack cases. The dataset should contain various data points, including both usual and unusual cases (or attacks and non-attacks), which will help the model learn to distinguish between them. The proposed data generation method involves two key steps: modelling of the PV farm and the threats model. These two steps are explained in detail in the following subsections.

#### Modelling of PV Farm

This section presents the design and implementation of the PV farm model to simulate real-world conditions when subjected to malicious activity attempts. The PV farm model design is implemented in MATLAB to simulate 2-MW PV farm, as shown in Figure 3. The design shows that the photovoltaic system and inverter are connected via a DC/DC connection to maximize the energy extracted from the PV array. Furthermore, the PV farm model connects two parallel inverters to an electrical grid with all the required systems for control. The PV panel model can be given by the dynamic equation of the V-I relationship as in Equations (1) and (2) [28]:

$$I_{\mathrm{PV}} = I_{\mathrm{PV}} - I_D - I_{Sh} \tag{1}$$

$$I_{\mathrm{PV}} = I_{\mathrm{PV}} - I_0 \times [exp\,[((Q \times V_D)/n \times k \times T - 1) - V_D/R_{Sh}]] \tag{2}$$

where the "$V_D$" is diode voltage, "$I_0$" is reverse saturation current, "$Q$" is for electron charge, "$n$" is the number of cells per module, "$k$" for Boltzmann factor, "$T$" represents the absolute temperature in Kelvin, "$I_{\mathrm{PV}}$" is PV current, "$I_D$" is diode current, and "$I_{Sh}$" is shunt resistor current.

The DC/DC converter is typically designed as the step-up converter. The ideal duty cycle for the step-up converter control is produced by the DC/DC regulator. The model of the step-up converter applied in Equations (3) and (4).

$$\dot{V}_{PV} = \frac{I_{PV} - I_L}{C_{PV}} \tag{3}$$

$$\dot{I}_L = \frac{\boldsymbol{V_{PV}} - (\mathbf{1} - \boldsymbol{D}) \times \boldsymbol{V_{DC}}}{\boldsymbol{L}} \tag{4}$$

where the $L$ stands for the DC/DC system inductor, "$D$" is the duty cycle, "$V_{DC}$" is the DC link capacitor's voltage, "$I_L$" is the inductance current, and "$I_{PV}$" and "$V_{PV}$" are the current and voltage of the PV farm.

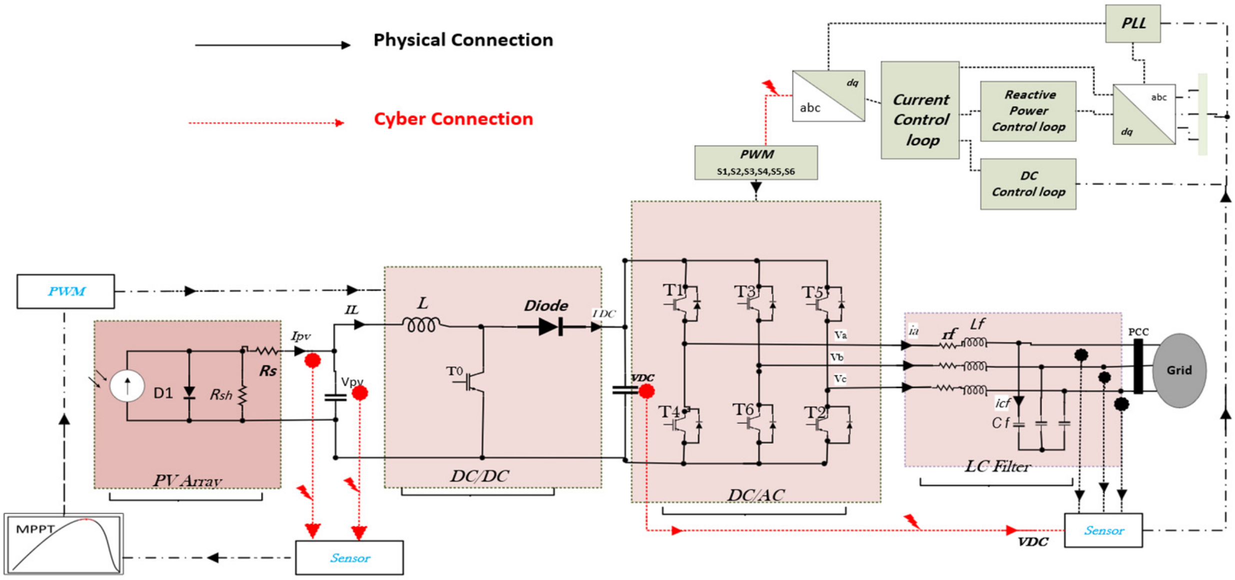


**Figure 3.** PV Farm System Configuration.

The association involving "$V_{PV}$ "and "$V_{DC}$" in a steady state may be calculated as follows Equation (5) [29]:

$$\frac{V_{DC}}{V_{\text{PV}}} = \frac{1}{1 - D} \tag{5}$$

The following Equation (6) are employed to represent the inverter and LC filter of the inverter in Equations (7)–(10) [26,30,31]:

$$\left.\begin{array}{r} V_a = V_{cf} + r_f I_a + L_f \dot{I}_a \\ L_f \dot{I}_a = -V_{cf} - r_f I_a + V_a \\ \dot{I}_a = -\frac{V_{cf}}{L_f} - \frac{r_f}{L_f} I_a + \frac{V_a}{L_f} \end{array}\right\} \tag{6}$$

While only Phase "$a$" is illustrated, Phases "$b$" and "$c$" follow similar mathematical formulations. The voltage of the phase "$a$" is $V_a$, the current of the phase "$a$" is $I_a$, $V_{cf}$ is the capacitor voltage in the filter circuit, $r_f$ represent the internal resistance of the filter, $\dot{I}_a$ representing the current rate of change over time and $L_f$ the inductance of the inductor in the filter.

The voltages and currents in regular distribution power networks should exhibit stability, as shown in the following Equation (7):

$$\left.\begin{array}{r} V_a = \frac{V_{Dc}}{3}(2S_a - S_b - S_c) \\ \dot{I}_a = -\frac{V_{Cf}}{L_f} - \frac{r_f}{L_f} i_a + \frac{V_{Dc}}{3L_f}(2S_a - S_b - S_c) \\ \dot{I}_b = -\frac{V_{Cf}}{L_f} - \frac{r_f}{L_f} i_b + \frac{V_{Dc}}{3L_f}(-S_a + 2S_b - S_c) \\ \dot{I}_c = -\frac{V_{Cf}}{L_f} - \frac{r_f}{L_f} i_c + \frac{V_{Dc}}{3L_f}(2S_c - S_b - S_a) \end{array}\right\} \tag{7}$$

where $\dot{i}_a, \dot{i}_b, \dot{i}_c$ are the current of each phase, $S_a, S_b, S_c$ are the switches of the three-phase inverter, which are the control signals.

$$\left.\begin{array}{r} U_{Cf} = V_g \\ I_a = I_g + I_{Cf} \\ I_a = I_g + C_f\,\dot{U}_{Cf} \end{array}\right\} \tag{8}$$

Transfer to dq_model

$$\left.\begin{array}{l} \dot{i}_d = -\frac{U_{Cfd}}{L_f} - \frac{r_f}{L_f} i_d - \omega\, i_q + \frac{V_{Dc}}{3L_f} S_d \\ \dot{i}_q = -\frac{U_{Cfq}}{L_f} - \frac{r_f}{L_f}\, i_q + \omega\, i_d + \frac{V_{Dc}}{3L_f} S_q \end{array}\right\} \tag{9}$$

$$\left.\begin{array}{l} i_{Cfd} = C_f\,\dot{U}_{Cfd} + C_f\,\omega\,U_{Cfq} \\ i_{Cfq} = C_f\,\dot{U}_{Cfq} - C_f\,\omega\,U_{Cfd} \end{array}\right\} \tag{10}$$

"$i_d$" and "$i_q$" are the system line currents of the grid in the d,q frame; "$U_{Cfd}$" and "$U_{Cfq}$" are the LC capacitor voltages in the d,q frame; and $V_{Dc}$ is the voltage of the dc link capacitor. "$I_f$" is the inductance current in the LC filter in the d,q frame.

### *7.2. Threats Model*

The issue of cyber-attacks affecting the electrical waveforms at the Point of Common Coupling (PCC) should be addressed due to their detrimental impact on the stability and integrity of the PV system. Specifically, when an unauthorized user gains access to the grid-connected PV farm asset, any changes to sensor readings can threaten the PV controller, can potentially destabilize the power grid. This instability may result in severe failures and substantial economic losses. To analyze these attacks on a PV farm, a threat model was designed to simulate potential cyber risks using a targeted attack vector based on the developed PV system model. The threat model specifically includes four attack scenarios targeting the integrity of PV data within the simulated PV model. To illustrate the impact of data integrity attacks (DIA) on output waveforms, two key components of the simulated PV farm system—the DC/DC converter and the DC/AC inverter—are subjected to these attacks. The parameters from sensors DC/DC and DC/AC controls collected as in Equation (11):

$$y(t) = [V_{PV}(t), I_{PV}(t), V_{DC}(t), I_f(t), U_C(t)]^{\boldsymbol{T}} \tag{11}$$

where "$V_{PV}(t)$, $I_{PV}(t)$" are the voltage and the current of the PV farm, "$V_{DC}(t)$" is the DC link voltage, "$I_f(t)$, $U_C(t)$" are the current and voltage of LC filter.

Table 2 explains four scenarios of DIA, which imposed two attacks on the DC/DC and the other on the DC/AC. The faked measurement ($y$^) and actual measurement ($y$) are modelled to illustrate cyber attacks on the sensor. Subsequently, the expression for the cyberattack that alters sensor input can be formulated as shown in Equation (12).

$$\boldsymbol{y}^{\wedge}(\boldsymbol{t}) = \propto \boldsymbol{y}(\boldsymbol{t} - \boldsymbol{t}_{\boldsymbol{delay}}) \tag{12}$$

where the $t \in$ T_attack, and the constrain of the weight of attack $\propto = \begin{cases} > 1 \\ < 1 \end{cases}$ for falsifying the original value of PV data. The attack vector of the current coefficients represents $\propto_{\mathrm{I}}$, and the attack vector of the voltage coefficients as $\propto_{\mathrm{V}}$ measuring in the photovoltaic panel.

**Table 2.** Threats description.

| Case of DIA | Description of Case |
|---|---|
| Attack case 1 | Modifying the inputs sensor of DC/DC control. |
| Attack case 2 | Alter the incremental value of the MPPT algorithm for the DC/DC controller. |
| Attack case 3 | Inject delay time to signal control of DC/AC |
| Attack case 4 | Modifying the VDC feedback sensor to DC/AC controller |

- **Attack case 1**

In this scenario, the attack seeks to manipulate or inject false data into the converter's control system by altering voltage and current measurements. In our threat model, these measurements serve as inputs to the DC/DC control (MPPT) and are targeted by the attacker. To modify or increase the input sensor value by setting the voltage $\propto_V \in (5, 0.2)$ and the current $\propto_I \in (3, 0.4)$, which affects the MPPT controller at 0.5 sec to simulate proper data entry. In this way, based on Equations (2), (3) and (5), the attack coefficients alter the original data, resulting in disturbances in the output waveform of current at the side of the grid (the PCC). The data collected from this attack scenario is labeled as "DC/DC1," with the PCC data derived from the waveform pattern observed during the attack, as shown in Figure 4.

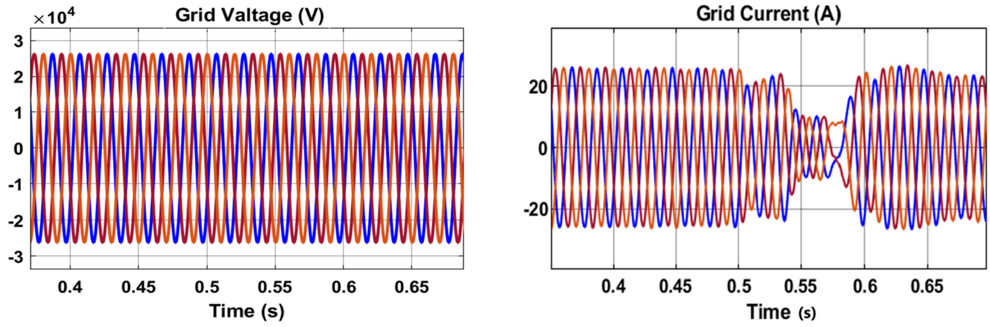


**Figure 4.** Attack case 1 against DC/DC at the side of the grid (voltage, current).

- **Attack case 2**

The second attack scenario involves altering data within the Maximum Power Point (MPP) control. This attack disrupts the current waveform by modifying the duty cycle in the MPP parameter (the incremental value used to adjust the duty cycle DD). The controller algorithm is manipulated to operate with an increment value exceeding its normal range. Typically, DD is set to 0.01 under standard conditions, but during the attack, this value is changed to 0.1, affecting the operation of the inverter and the entire system, as described in Equation (5). In this scenario, "DC/DC2" represents the collected data, illustrated in Figure 5.

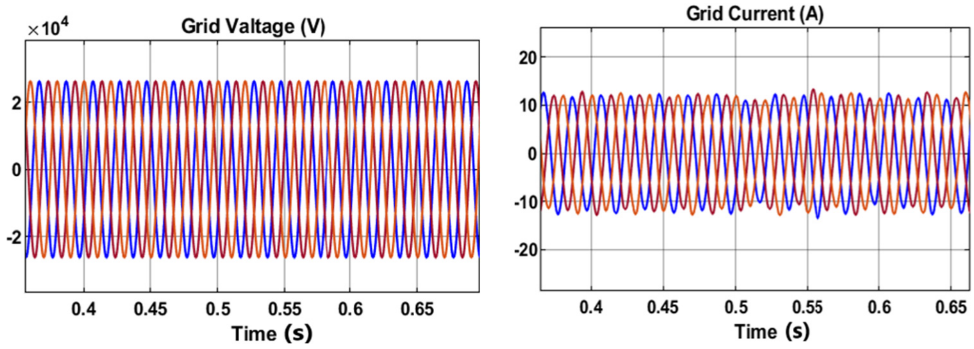


**Figure 5.** Attack case 2 against DC/DC at the side of the grid (voltage, current).

- **Attack case 3**

In this scenario, an attack introduces a delay in the DC/AC inverter. This attack targets the inverter control signal, inadvertently delaying the feedback of the DC/AC inverter. The delay generates harmonics in the system, as described by Equation (10), which degrades the controller's performance. To simulate this attack, a 10 ms delay is applied to the control signal, as depicted in Figure 6. The data collected from this attack, labeled "DC/AC1", is subsequently input into the deep learning algorithms.

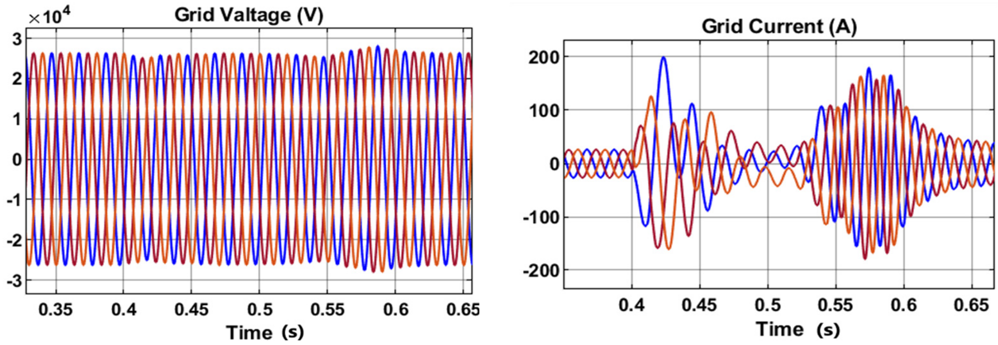


**Figure 6.** Attack case 3: Voltage and current waveforms during attack 3 at DC/AC inverter.

- **Attack case 4**

The final attack targets the feedback from the VDC sensor in the inverter control, causing incorrect data to be merged with the correct data according to Equation (9). When the attack vector is set to 0.6, this results in the VDC being higher than its actual value, which then affects the voltage and current patterns on the grid side. This is reflected in Figure 7, which illustrates the attack on the DC/AC converter. The information gathered from this attack scenario was called "DC/AC2" and used as input for the deep learning algorithm.

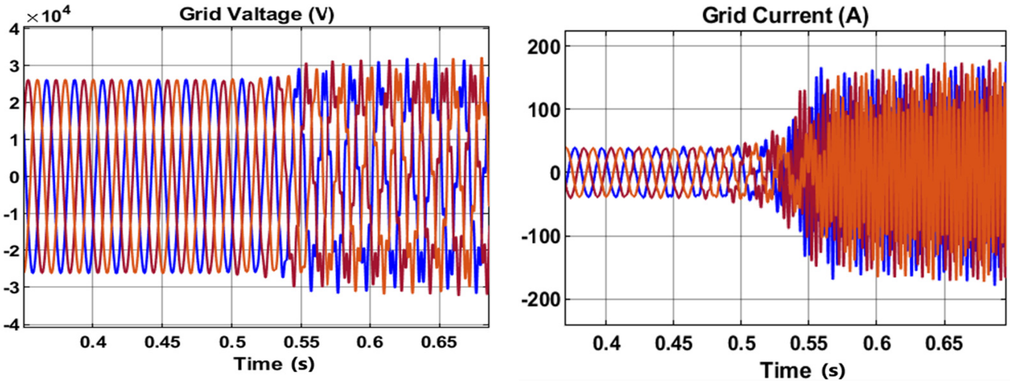


**Figure 7.** Voltage and Current waveforms during attack 4 at DC/AC inverter.

**Normal operations:** All the attack scenarios mentioned above are compared with the system's normal operation data. The dataset collected during normal operation, which uses a single voltage and a single current sensor, is based on the current and voltage waveforms at the PCC for the system. The waveform sensor at the PCC was assumed to be reliable and secure, as shown in Figure 8. The term "normal" refers to the data collected during standard operations, which were used as inputs for the deep learning algorithms in all cases.

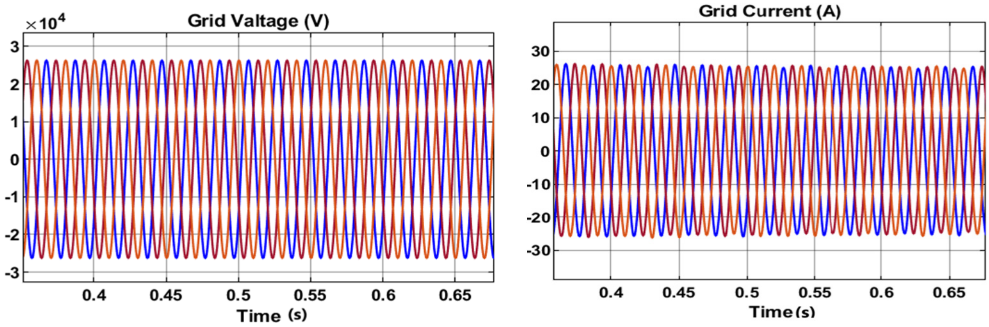


**Figure 8.** Voltage and current waveforms during normal operation condition.

This section presents the waveform results for each condition and the impact attack information on the system. In the AC power grid, the waveform sensors provide data on the three-phase current [I] = [Ia, Ib, Ic] and the recorded three-phase voltage [V] = [Va, Vb, Vc] at the connection point (PCC).

Effective detection and diagnosis of attacks at a high sample rate used to implement power electronic converters in photovoltaic (PV) farms. Electrical waveforms provide more significant benefits for detecting cyber attacks [27]. Every instance of sampling time yielded a data vector with six dimensions, denoted by Equation (13) which is used at the PCC of the inverter [32].

$$\mathrm{X^{wf}}_{\mathrm{t}} = [\,\mathrm{Va},\ \mathrm{Vb},\ \mathrm{Vc},\ \mathrm{Ia},\ \mathrm{Ib}, \mathrm{Ic}]^{\mathrm{T}} \tag{13}$$

where ($^{\mathrm{wf}}$) represents the observed normal waveform data for AC power grids, typically modeled as sinusoidal functions, to analyze the impact of various attacks on the waveform. Since the system operates in a stable state, the formulas for all three phases are identical. Consequently, using only the current and voltage of phase (a) provides essential tracking information, including the waveform's magnitude, phase angle, and frequency, which are the features collected over time. A data column is generated following Equation (14).

$$\boldsymbol{X^{wf}}_t = [\,M_{Va}, F_{Va}, \theta_{Va}\ , M_{Ia}\ , F_{Ia}, \theta_{Ia}]^{\boldsymbol{T}} \tag{14}$$

where $M_{Va}$ and $M_{Ia}$ represent the mean value of the one-phase of the voltage and the current, respectively. The frequency of phase (a) voltage and current are $F_{Va}, F_{Ia}$, phase angle of current and voltage are $\theta_{Va}, \theta_{Ia}$. So, the data collected from five classes (four attacks and routine operation) includes seven features over time. These features are continuous, and the dataset size for training is 7 × 22,819. To the best of our knowledge, this is the first attempt to use data from a single phase instead of all three phases of current and voltage. The collected data is shown in Table 3.

**Table 3.** The data collected from each class.

| Class | Name Data |
|---|---|
| Normal operation | Normal |
| Attack case 1 | DC/DC1 |
| Attack case 2 | DC/DC2 |
| Attack case 3 | DC/AC1 |
| Attack case 4 | DC/AC2 |

### *7.3. SMOTE (Synthetic Minority Over-Sampling Technique)*

After generating the dataset, the SMOTE technique is applied. SMOT addresses the class imbalance in the dataset by creating synthetic examples of the minority class (in this case, unusual or attack cases). This ensures that the model does not become biased towards the majority class (usual or non-attack cases) and improves its ability to detect the minority class effectively. This technique is essential to ensure high performance of attack detection and diagnosis due to the outperformance of simple oversampling, and it is often used to enhance randomized oversampling [33].

Figure 9 shows the class distribution of attacks in the dataset, with corresponding percentages assigned based on the fact that some attacks are restricted to specific periods during the electrical system's operation in each case. Class distribution results revealed that some classes have very large rate sampling, such as Normal and DC/DC2 data, and others have less rate sampling than DC/AC1 data. This distribution refers to the class data imbalance which helps to assess the impact of the attack on the electrical system's performance. When entering data without SMOTE into any algorithm for training data and testing data, it tends to use the high-rate data of the class, causing oversampling. It neglects low-rate class data, which causes a decrease in the accuracy of the results and failure to detect attacks with low rates.

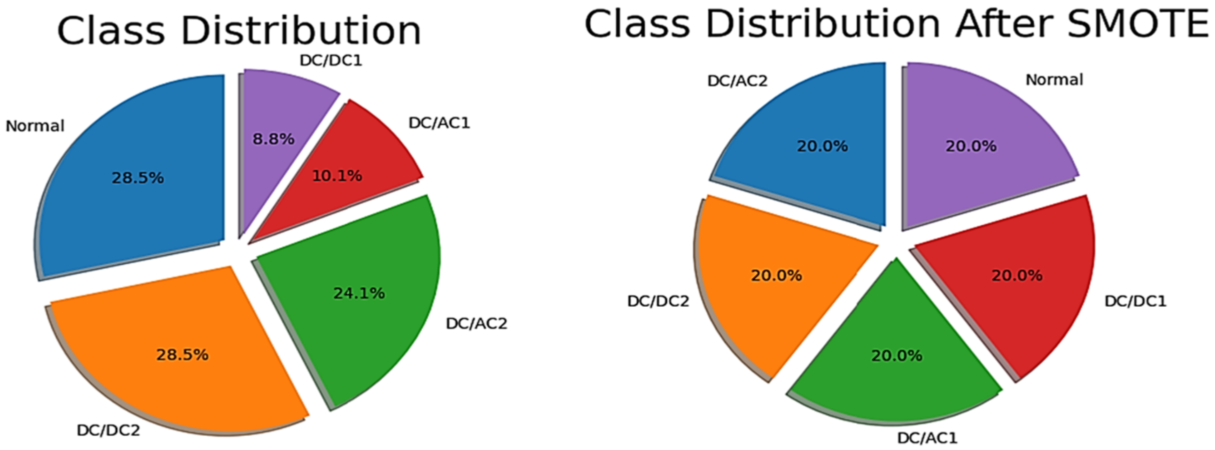


**Figure 9.** Class distribution before and after using SMTOE.

The right image of Figure 9 illustrates the balanced distribution of the five classes after applying SMOTE, with each class receiving an equal share of 20%. This indicates that SMOTE effectively ensures an even distribution of data across all classes, resulting in a more balanced dataset.

### 7.4. Preprocessing

In this step, the dataset is preprocessed to prepare it for model training. The preprocessing process involves tasks such as normalizing or standardizing the data, handling missing values, and encoding categorical variables. This step ensures the data is clean, consistent, and in the correct format for the model to process.

- We began by eliminating the unexpected distortion introduced by the SIMULINK simulation at the start of the data sample, as it could have led to inaccurate results.
- We normalized all collected data to the range [0,1] using the Z-score, due to the wide range of values across different features. For instance, the voltage value exceeds 23 kV, while the frequency is 50 Hz.

### 7.5. Training Dataset

Once the dataset is preprocessed, it is split into training and testing sets. The training dataset is the portion of the data used to train the model, allowing it to learn the patterns and relationships between features that indicate usual and unusual (attack) cases.

Using this method, we can estimate the generalization performance and determine the model hyperparameter. The training set is the primary dataset utilized for training and adjusting the model's parameters, including 80% of the datasets employed in the training procedure. In contrast, the testing set usually consists of the smallest dataset, with 20% allocated for the testing procedure.

### *7.6. CNN, MLSTM, ANN (Convolutional Neural Network, Multilayer Long Short-Term Memory, Artificial Neural Neural Network)*

In this step, the pre-processed and balanced training data is fed into three different types of neural networks. The proposed model's intrinsic difficulty means that each approach may address the issue with a varied processing capacity.

- **CNN (Convolutional Neural Network)**: Typically used for image and spatial data. CNNs can also be applied to time-series or structured data to capture spatial or local patterns because of their structural hierarchy, robust extracted feature capabilities, and ability to extract detailed, insightful characteristics. As shown in Algorithm 1, A time series data sample of a certain length may be inputted into a (CNN) like an image by converting it into a matrix [34].

**Algorithm 1:** CNN method

```
Initialize CNN filters, weights, and biases
    For each epoch:
    For each data sample:
        # Convolution Layer
        For each filter:
            convolved_output = apply_filter(input_data, filter)
        # Pooling Layer
            pooled_output = max_pooling(convolved_output)
        # Flatten Layer
            flattened_output = flatten(pooled_output)
        # Fully Connected Layer
            output = softmax(weights * flattened_output + bias)
        # Calculate error (loss function)
            error = target − output
        # Backpropagation
        For each layer:
            gradient = error * derivative_of_activation_function
            Update filters, weights, and biases using gradient descent
    Repeat until convergence
Output: Attack detection classification (normal/attack)
```

- **MLSTM (Multilayer Long Short-Term Memory)**: An LSTM is a recurrent neural network (RNN) which is effective for sequence prediction. MLSTM refers to using multiple LSTM layers to better capture temporal dependencies in the data. As shown in Algorithm 2, It was created to offer a means of transferring historical data between time steps to address the disappearing gradient problem of RNN. In our work, data is cached for subsequent use to avoid the progressive disappearance of previous training data. Due to its versatility, LSTM can handle complete data sequences, particularly time-series data and single information points [35].

**Algorithm 2:** MLSTM method

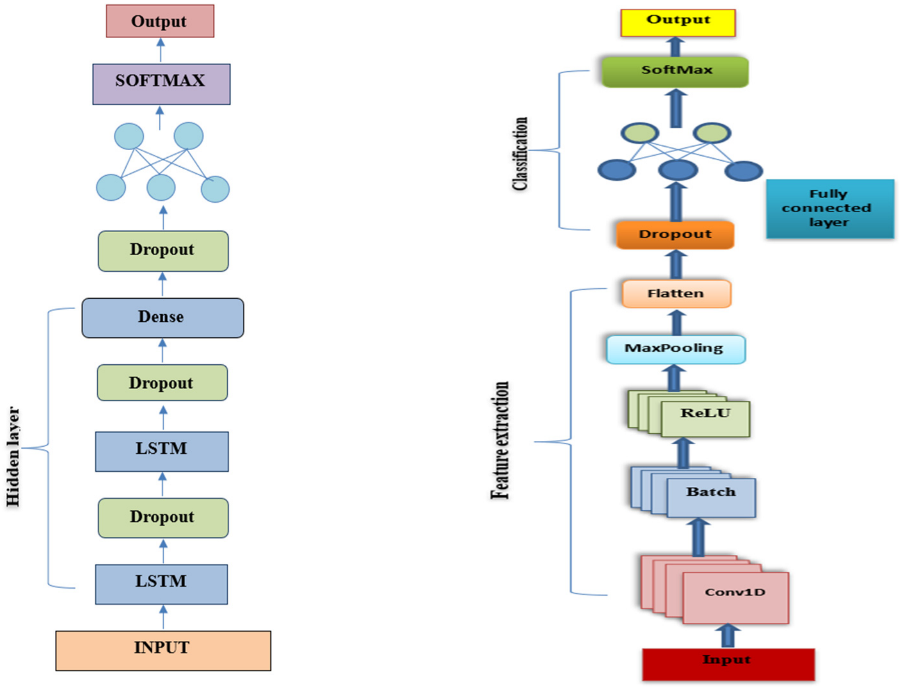
```
Initialize MLSTM cells with weights and biases for each input feature
For each epoch:
    For each time step in the multivariate data sequence:
        input_t = data_at_time_t (for each feature)
        prev_hidden_state = previous_hidden_state
        prev_cell_state = previous_cell_state

        # LSTM Computation for each feature
        Forget_gate = sigmoid(weights_f * input_t + bias_f)
        Input_gate = sigmoid(weights_i * input_t + bias_i)
        Cell_gate = tanh(weights_c * input_t + bias_c)

        # Update cell state and hidden state
        cell_state = Forget_gate * prev_cell_state + Input_gate * Cell_gate
        hidden_state = tanh(cell_state) * Output_gate

        # Output Classification
        output = softmax(weights_o * hidden_state + bias_o)

        # Calculate error (loss function)
        error = target − output

        # Backpropagation through time (BPTT) for each feature
        For each time step (from end to start):
            gradient = error * derivative_of_output_function
            Update MLSTM weights using BPTT

Repeat the training process until convergence (loss is minimized)

Output: Attack detection classification (normal/attack)
```

- **ANN (Artificial Neural Network)**: ANN is used for classification and regression tasks, learning from the training data to make predictions. Serving as the foundation of deep learning. ANN may employ any data that can be converted to a numeric format. A high number of inputs and nonlinear data make for an effective model. While ANN works well for basic problems, it is typically utilized as the output layer of an additional sophisticated network when the issue becomes deeper [36], see Algorithm 3. These networks work together or individually to learn complex patterns in the data, allowing the model to differentiate between usual and unusual activities.

Figures 10a and 10b respectively illustrate the structures of the deep learning methods, including the CNN and LSTM models, used in this work. The most crucial factor of CNN, LSTM, and ANN models is hypermeters, which also affect the performance of these models like accuracy and speed converges. Furthermore, these hypermeters are contained in Table 4, which is used in deep learning methods adopted in this work.

**Algorithm 3:** ANN method

```
Initialize network weights and biases
For each epoch:
    For each data sample:
        # Forward Propagation
        input = data_sample
        For each layer:
            output = activation(weights * input + bias)
            input = output
        # Calculate error (loss function)
        error = target − output
        # Backpropagation
        For each layer (starting from the output layer):
            gradient = error * derivative_of_activation_function
            Update weights and biases using gradient descent
Repeat until convergence (loss is minimized)
Output: Attack detection classification (normal/attack)
```



(**a**) (**b**)

**Figure 10.** The architecture for classified data using (**a**) LSTM (**b**) CNN.

**Table 4.** The hyperparameter description .

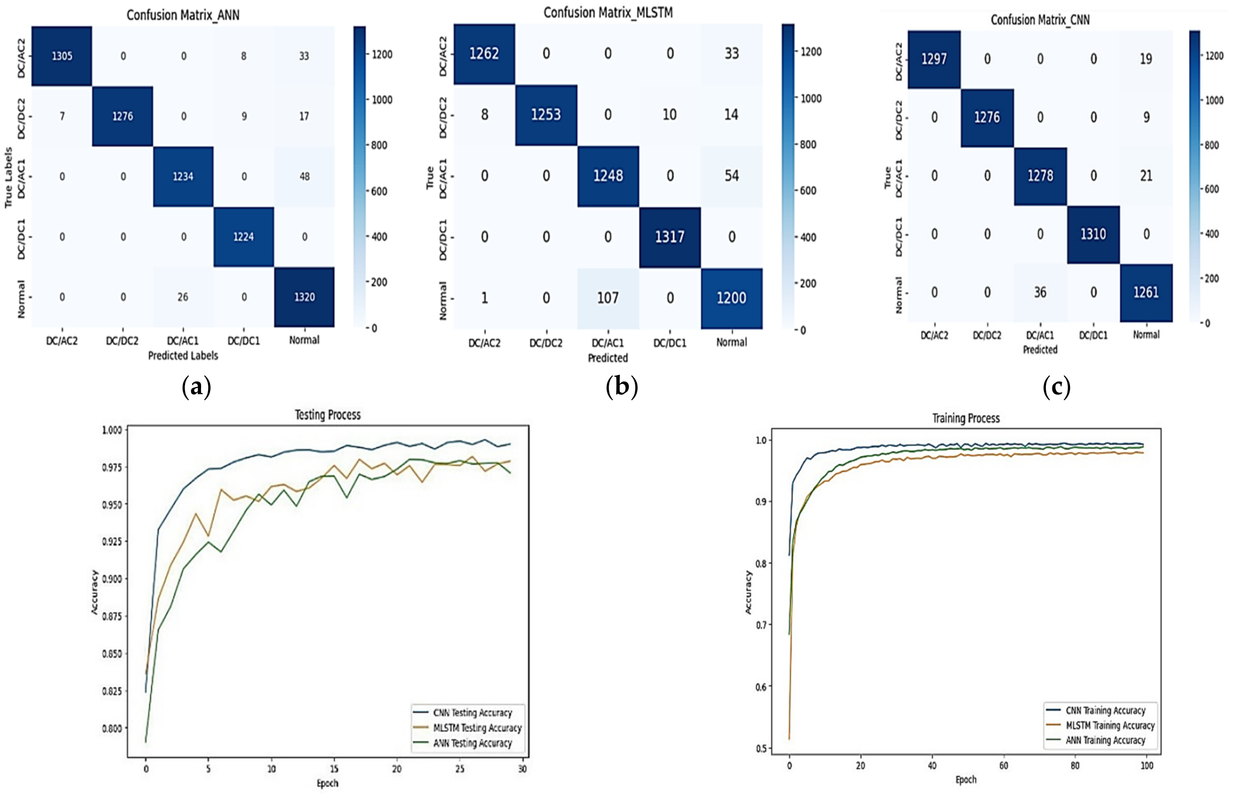
| Hypermeters | CNN | LSTM | ANN |
|---|---|---|---|
| Bach size | 32 | 32 | 32 |
| learning rate | 0.001 | 0.001 | 0.001 |
| the number of layers | 4 | 4 | 3 |
| Input activation function | ReLU | ReLU | ReLU |
| output activation function | SoftMax | SoftMax | SoftMax |
| Kernel size | 2 | - | - |
| Number of Dropouts | 1 | 3 | - |
| Max pooling layer | 1 |  | - |
| Fully connected layer | 1 | 2 | 3 |

### 7.7. Classification of Attack (Usual, Unusual)

Recognizing the occurrence of an attack is crucial, but identifying multiple simultaneous attacks can be challenging. While many studies focus on attack diagnosis and detection by splitting data into two categories (normal and abnormal) for binary classification, this study adopts multiclass classification to achieve higher detection performance. The data is divided into five categories: normal, DIA in DC/AC controllers 1 and 2, and DIA in DC/DC controllers 3 and 4. For attack diagnosis, the categorical_crossentropy loss function is used to accurately identify different types of attacks, enabling fast diagnostic and classification tasks [37]. This approach handles large datasets (over 200 k samples), in contrast to research studies that use smaller, lower-rate sampling.

## 8. Results

The experimental findings are shown in Figure 11a–e. The results show that by using the confusion matrix to visually analyze each model, we can effectively assess and achieve optimal attack detection and precise diagnosis of attack classes. The confusion matrix enables a comparison between the actual class labels (representing the true types of attacks) and the predicted labels, providing valuable insights. It offers a visual representation of accurate attack detection. The diagonal cells in the matrix represent correct identifications of attacks or normal conditions, while the off-diagonal elements indicate misclassifications. The y-axis represents the predicted labels, and the x-axis represents the true labels, as shown in Figure 11a–c.



(**a**) (**b**) (**c**)

(**d**) (**e**)

**Figure 11.** Detection and diagnosis of attacks using (**a**) ANN, (**b**) LTSM, (**c**) CNN, (**d**) testing process, and (**e**) training process.

All models demonstrated high detection accuracy, with most predictions matching the actual attack categories. For example, the CNN model exhibited exceptional performance in identifying attacks, with only a few instances of misclassification. The confusion matrix for the ANN model, a basic neural network structure, accurately identified most scenarios but showed some misclassifications between the "normal" class and certain attack categories, indicating incorrectly flagged attacks.

Figure 11d,e show the ROC curves for the three model methods, each requiring 100 epochs for training and 30 epochs for testing. It is evident that the CNN model demonstrated highly efficient performance due to its neural network architecture, which processes input data through convolutional layers that extract local features and share weights. This results in significantly better performance compared to other artificial intelligence models like ANNs and LSTMs. Comparatively, Table 5 shows that CNN performs better than all other models across the board (accuracy of 98.4939%). We attribute this to its potent feature extraction and latent information extraction capabilities. This indicates that CNN is capable of processing big data in addition to its exceptional image processing skills.

**Table 5.** Detection efficiency by applying the metrics evaluation method.

| **Model\Metrics** | ***Accuracy*** | ***Precision*** | ***Recall*** | ***F1*** |
|---|---|---|---|---|
| ANN | 96.1733 | 96.3256 | 96.2079 | 96.2115 |
| LSTM | 96.5114 | 96.5259 | 96.5114 | 96.5259 |
| CNN | 98.4939 | 98.5575 | 98.4939 | 98.50295 |

On the other hand, Table 6 presents the detection time per epoch for the three models. Both CNN and MLSTM demonstrated faster prediction processes, achieving results in a shorter time compared to the ANN model. However, deep learning techniques continue to outperform other approaches, with the performance gap widening as the situations become more complex. It is important to note that LSTM is well-known for its ability to effectively handle time-series data due to its superior memory capabilities. However, surprisingly, the ANN model outperforms LSTM in both performance and stability. This may be because the time-series data in this case is relatively simple, limiting LSTM's ability to fully demonstrate its advantages.

**Table 6.** Detection time.

| **Model** | **Time (s)** |
|---|---|
| ANN | 2.39 |
| LSTM | 1.69 |
| CNN | 1.47 |

To assess the performance of the strategy, we use accuracy, precision, recall, and F1-scores derived from the confusion matrix as detection and classification metrics, as shown in Table 5. The four values from the confusion matrix are True Negative (*TN*), False Negative (*FN*), True Positive (*TP*), and False Positive (*FP*). The metrics are defined by the following Equations (15)–(18):

$$Accuracy = \frac{TN + TP}{TN + TP + FP + FN} \tag{15}$$

$$Precision = \frac{TP}{TP + FP} \tag{16}$$

$$Recall = \frac{TP}{TP + FN} \tag{17}$$

$$F1_{SCORES} = \frac{2TP}{2TP + FP + FN} \tag{18}$$

## 9. Conclusions

To guarantee reliable power system operation, smart grid security concerns require greater attention. A new cyber detection model in PV, named as CDPV, is introduced in this paper. To determine how DIA affects different control mechanisms in a PV operation system utilizing the MATLAB Simulink to generate the dataset, this paper looks at both mathematical evaluations and case studies. First, DIA on the solar energy farm incorporated into the distributed energy system was examined. A PV system converter with two stages is created, and the DIA model is constructed for validation. This research presents theoretical evaluation and case studies to ascertain the consequences of DIA. This study examines several forms of database intrusions in this work and creates five distinct datasets with both attack and normal occurrences. Then, the different rates of samples for each case create a challenge to avoid excessive bias in data for one case over the other SMOTE used, which contributes to supporting more accurate evaluations of deep learning techniques, especially through the use of multi-class classification at a high sample rate of the wave to improve the accuracy of attack detection. Then, three data-driven approaches are compared: ANN, CNN, and LSTM. The results of this study show that the CNN performs better than all other models with a high accuracy of 98.4939%. The suggested technique has been tested using Google Colab and has significantly better attack detection and diagnostic capabilities. The futur work of the paper involves detecting cyber and physical attacks in photovoltaic farms integrated with IEEE bus systems, addressing challenges like solar energy variability and grid integration using advanced machine learning techniques. Simulations will be conducted to ensure robustness and contribute to renewable energy security in smart grids.

**Author Contributions:** G.F.H.: Conceptualization; Methodology; Software; Validation; Investigation; Resources; Data curation; Writing—original draft preparation; Visualization; Project administration; Writing—review and editing. M.S.: Investigation, Conceptualization, Funding acquisition, Project administration Data curation, Writing—original draft preparation, Writing—review & editing. O.A.A.: Visualization, Data curation, Resources, Writing—original draft preparation. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Data is contained within the article.

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

## References

1. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**, *9*, 5326–5340. [CrossRef]
2. Aslam, A.; Ahmed, N.; Qureshi, S.A.; Assadi, M.; Ahmed, N. Advances in Solar PV Systems; A Comprehensive Review of PV Performance, Influencing Factors, and Mitigation Techniques. *Energies* **2022**, *15*, 7595. [CrossRef]
3. Moses, J.B.; Oludolapo, A.O. Smart grid technologies and application in the sustainable energy transition: A review. *Int. J. Sustain. Energy* **2023**, *42*, 685–758.
4. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.S. A Review of Cyber–Physical Security for Photovoltaic Systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *10*, 4879–4901. [CrossRef]
5. Hasan, G.; Dilan, J. Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems. *Int. J. Electr. Power Energy Syst.* **2018**, *101*, 371–384.
6. Ehsan, M.A. Cybersecurity Challenges in Distributed Control. Systems and Control (eess.SY). *arXiv*, 2021; arXiv:2106.13712.
7. Khalil, S.M.; Bahsi, H.; Ochieng, H.; Korõtko, T.; McLaughlin, K.; Kotkas, V. Threat Modeling of Cyber-Physical Systems—A Case Study of a Microgrid System. *Comput. Secur.* **2023**, *124*, 102950. [CrossRef]
8. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163 Pt A*, 396–412. [CrossRef]

9. Yohanandhan, R.V.; Elavarasan, R.M.; Pugazhendhi, R.; Premkumar, M.; Mihet-Popa, L.; Zhao, J.; Terzija, V. A specialized review on the outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. *Int. J. Electr. Power Energy Syst.* **2022**, *136*, 107720. [CrossRef]
10. Alnajim, A.M.; Habib, S.; Islam, M.; Thwin, S.M.; Alotaibi, F. A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. *Technologies* **2023**, *11*, 161. [CrossRef]
11. Mohamed, S.; Abd El Sattar, M. A comparative study of P&O and INC maximum power point tracking techniques for grid-connected PV systems. *SN Appl. Sci.* **2019**, *1*, 174.
12. Saxena, A.; Kumar, R.; Amir, M.; Muyeen, S.M. Maximum power extraction from solar PV systems using intelligent based soft computing strategies: A critical review and comprehensive performance analysis. *Heliyon* **2024**, *10*, e22417. [CrossRef] [PubMed]
13. Meshram, D.K.; Goel, N.; Chacko, S. Integration of Battery Energy Storage System with Solar Power Generation System along with Load Management System. In Proceedings of the 2022 International Conference for Advancement in Technology (ICONAT), Goa, India, 21–22 January 2022; pp. 1–8.
14. Aghaei, M.; Fairbrother, A.; Gok, A. Review of degradation and failure phenomena in photovoltaic modules. *Renew. Sustain. Energy Rev.* **2022**, *159*, 112160. [CrossRef]
15. 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]
16. Barua, A.; Al Faruque, M.A. Special Session: Noninvasive Sensor-Spoofing Attacks on Embedded and Cyber-Physical Systems. In Proceedings of the 2020 IEEE 38th International Conference on Computer Design (ICCD), Hartford, CT, USA, 18–21 October 2020; pp. 45–48.
17. Strezoski, L.; Babic, Z.; Milojicic, D. Cyber Physical Security of Distributed Energy Resources. *Energy* **2023**, *XXV*, 1–9.
18. Kumari, R.; Prabhakaran, K.K.; Chelliah, T.R. Improved Cybersecurity of Power Electronic Converters Used in Hydropower Plant. In Proceedings of the 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020; pp. 1–6.
19. Balda, J.C.; Mantooth, A.; Blum, R.; Tenti, P. Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things. *IEEE Power Electron. Mag.* **2017**, *4*, 37–43. [CrossRef]
20. Harrou, F.; Taghezouit, B.; Bouyeddou, B.; Sun, Y. Cybersecurity of photovoltaic systems: Challenges, threats, and mitigation strategies: A short survey. *Front. Energy Res.* **2023**, *11*, 1274451. [CrossRef]
21. Li, F.; Xie, R.; Yang, B.; Guo, L.; Ma, P.; Shi, J.; Ye, J.; Song, W.Z. Detection and Identification of Cyber and Physical Attacks on Distribution Power Grids with PVs: An Online High-Dimensional Data-Driven Approach. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 1282–1291. [CrossRef]
22. Ramos-Ruiz, J.; Kim, J.; Ko, W.H.; Huang, T.; Enjeti, P.; Kumar, P.R.; Xie, L. An Active Detection Scheme for Cyber Attacks on Grid-tied PV Systems. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6. [CrossRef]
23. Sabeur, Z.; Bruno, A.; Johnstone, L.; Ferjani, M.; Benaouda, D.; Arbab-zavar, B.; Cetinkaya, D.; Sallal, M. Cyber-Physical Behaviour Detection and Understanding using Artificial Intelligence. 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022), New York, NY, USA, 24–28 July 2022.
24. Li, Q.; Li, F.; Zhang, J.; Ye, J.; Song, W.; Mantooth, A. Data-driven Cyberattack Detection for Photovoltaic (PV) Systems through Analyzing Micro-PMU Data. In Proceedings of the 2020 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA, 11–15 October 2020; pp. 431–436.
25. Zhang, J.; Li, Q.; Ye, J.; Guo, L. Cyber-physical security framework for photovoltaic farms. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–7.
26. Li, F.; Li, Q.; Zhang, J.; Kou, J.; Ye, J.; Song, W.Z.; Mantooth, H.A. Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network. *IEEE Trans. Power Electron.* **2021**, *36*, 2495–2498. [CrossRef]
27. Zhang, J.; Guo, L.; Ye, J.; Giani, A.; Elasser, A.; Song, W.; Liu, J.; Chen, B.; Mantooth, H.A. Machine Learning-Based Cyber-Attack Detection in Photovoltaic Farms. *IEEE Open J. Power Electron.* **2023**, *4*, 658–673. [CrossRef]
28. Pushpa, K.R.; Bethany, R.S. Mathematical model and analysis of PV Converter—Inverter System. *Mater. Sci. Eng.* **2021**, *1187*, 012019. [CrossRef]
29. Madhukumar, M.; Suresh, T.; Jamil, M. Investigation of Photovoltaic Grid System under Non-Uniform Irradiance Conditions. *Electronics* **2020**, *9*, 1512. [CrossRef]
30. Hasan, F.A.; Rashad, L.J.; Humod, A.T. Integrating Particle Swarm Optimization and Routh-Hurwitz's Theory for Controlling Grid-Connected LCL-Filter Converter. *Int. J. Intell. Eng. Syst.* **2020**, *13*, 102–113. [CrossRef]
31. Oleiwi, S.S.; Humod, A.T.; Hasan, F.A. Injected power control for grid-connected converter based on particle swarm optimization. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *27*, 1199–1211. [CrossRef]
32. Sarker, I.H. Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Comput. Sci.* **2021**, *2*, 420. [CrossRef] [PubMed]

33. Blagus, R.; Lusa, L. SMOTE for high-dimensional class-imbalanced data. *BMC Bioinform.* **2013**, *14*, 106. [CrossRef] [PubMed]
34. Van Houdt, G.; Mosquera, C.; Nápoles, G. A review on the long short-term memory model. *Artif. Intell. Rev.* **2020**, *53*, 5929–5955. [CrossRef]
35. Yamashita, R.; Nishio, M.; Do, R.K.G.; Togashi, K. Convolutional neural networks: An overview and application in radiology. *Insights Imaging* **2018**, *9*, 611–629. [CrossRef] [PubMed]
36. Richmond, A. A Brief Introduction to Artificial Neural Networks. Available online: http://tuxar.uk/brief-introduction-artificial-neural-networks/ (accessed on 1 May 2024).
37. Zhang, Z.; Sabuncu, M. Generalized cross entropy loss for training deep neural networks with noisy labels. *Adv. Neural Inf. Process. Syst.* **2018**, *31*.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.