IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 December 2023, accepted 24 December 2023, date of publication 1 January 2024,
date of current version 9 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3348549

RESEARCH ARTICLE

A Deep Convolutional Neural Network-Based Approach to Detect False Data Injection Attacks on PV-Integrated Distribution Systems

MASOUD AHMADZADEH[1], AHMADREZA ABAZARI[1], (Member, IEEE), MOHSEN GHAFOURI[1], (Member, IEEE), AMIR AMELI[2], (Member, IEEE), AND S. M. MUYEEN[3], (Fellow, IEEE)

[1]Security Research Center, Concordia University, Montreal, QC H3G 1M8, Canada
[2]Electrical Engineering Department, Lakehead University, Thunder Bay, ON P7B 5E1, Canada
[3]Department of Electrical Engineering, Qatar University, Doha, Qatar

Corresponding author: S. M. Muyeen (sm.muyeen@qu.edu.qa)

Open Access funding provided by the Qatar National Library.

ABSTRACT The integration of photovoltaic (PV) panels has allowed power distribution systems (PDSs) to regulate their voltage through the injection/absorption of reactive power. The deployment of information and communication technologies (ICTs), which is required for this scheme, has made the PDS prone to various cyber threats, e.g., false data injection (FDI) attacks. To counter these attacks, this paper proposes a data-driven framework to detect FDI attacks against voltage regulation of PV-integrated PDS. Initially, an attack-free system is modeled along with its voltage regulation scheme, where the grid measurements are sent to a centralized controller and the control signals are transmitted back to PVs to be used by their local controllers. Then, a convolutional neural network (CNN) framework is proposed to detect FDI attacks. To train this framework—which should be able to distinguish between normal grid behaviors and attacks—a complete and realistic dataset is formed to cover all normal conditions and unpredictable changes of a PDS during a year. Since normal variations and fluctuations in power consumption lead to changes in the voltage profile, this dataset is enriched using features such as season, weekdays, weekends, load conditions, and PV generation power. The performance of the trained framework has been compared with other supervised Machine Learning-based and deep-learning techniques for FDI attacks against modified IEEE 33- and 141-bus PDSs. Simulation results demonstrate the superior performance of the proposed framework in detecting FDI attacks.

INDEX TERMS Distribution systems, false data injection, cyberattacks, convolutional neural network, photovoltaic, voltage regulation.

I. INTRODUCTION

To improve the efficiency of power distribution systems (PDSs), renewable energy sources, e.g., solar and wind, have been extensively incorporated into the grid [1]. Among these renewable energies, Photovoltaic (PV) systems have received a high level of consideration due to their efficacy, low maintenance requirements, and being a viable source of renewable energy [2], [3]. The deployment of PVs not only generates electricity but also brings other benefits to PDSs, for instance, by injection/absorption of reactive power, which enables the grid to regulate voltage within acceptable

The associate editor coordinating the review of this manuscript and approving it for publication was Fabio Mottola.

ranges [4], [5]. In a PV-integrated PDS, voltage readings are sent to a centralized controller to manage voltage levels at a specific location, such as the point of common coupling (PCC). The controller then calculates control signals that are sent back to the PVs, where they are added to the local control loops of the PV converters [6]. To have such a voltage regulation scheme, the central controller and PVs need to transfer data and commands, which consequently requires the use of information and communication technologies (ICTs). Such a deployment, however, makes the entire voltage regulation scheme vulnerable to various cyberattacks [7], [8], [9], among which false data injection (FDI) attacks received significant attention due to their easy execution and severe impact on the performance of PDSs [10], [11], [12]. Furthermore, the real-time nature of control systems makes it difficult to detect and mitigate FDI attacks in a timely manner. Thus, it is of paramount importance to design effective detection mechanisms for protecting PV-integrated PDSs against FDI attacks [13], [14].

Recently, a literature survey has been provided to investigate the existing challenges associated with distribution system state estimation and cyber intrusions that mainly focus on the impacts of FDI attacks, along with developing the co-simulation platform for investigation of the vulnerability of cyber-physical systems [15]. In another literature survey, it is concluded that existing detection algorithms, which have been developed for cyber attack purposes in distribution networks, can be classified into two different groups: (i) model-based approaches, and (ii) data-based approaches [16]. A novel FDI attack against the voltage regulation of PDS connected to EV loads has been investigated in [17] to demonstrate the impacts of such attacks on voltage stability. Moreover, the potential for a cyber attack on the measurement signals, that integrate volt-var control (VVC) in next-generation distribution networks, has been studied in [18]. Since attackers tend to be stealthy during cyber attacks, a game-theoretic framework is defined where system operators can adjust proper settings to maximize observability with the aim of limiting the adversary action space. In another work [19], the impact of cyber attacks on voltage regulation in PDS connected to photovoltaic systems has been studied. These attacks have been created by falsifying sensor measurements obtained from separating switches that can be transmitted to the centralized control framework in the PDS. On this basis, a simple detection algorithm is developed whose parameters can be calculated based on the system behavior under normal conditions [19]. Another mathematical model, e.g., state estimation approaches, can also be deployed for the detection of FDI attacks in distribution systems [20]. Despite the effectiveness of model-based methods, they suffer from several issues, such as requiring accurate knowledge about the parameters of underlying systems, which may not be accurately available [21]. Moreover, the designed detection frameworks are generally restricted to an operational range, which can result in non-optimal performance during different uncertainties in PDSs [22].

On the other hand, a group of other researchers has recently deployed machine learning (ML) techniques for real-time detection of different types of cyber-attacks in smart grids [23], [24], [25], [26]. For example, a learning method, that uses a time-series algorithm based on neural networks, i.e., a discrete-time nonlinear auto-regressive neural network with exogenous inputs, has been suggested to detect FDI attacks on the distribution infrastructure and mitigate their impacts accordingly. Another study suggests a deep learning-based framework, i.e., Multi-layer Long Short-Term Memory Network (MLSTM), for detecting cyber attacks in active PDS using voltage and current measurements [27]. Furthermore, in another work [28], authors have developed a two-stage technique that combines machine learning methods, i.e., Random Forest (RF) and Logistic Regression (LR), to detect and locate cyber attacks on control systems with the intent of regulating voltage in PDSs with distributed generators. In the mentioned work, first, the authors customize an RF regression method that uses previous voltage measurements and weather data to predict current voltage levels. Afterward, an LR-based method is developed to compare the predicted voltage levels with the actual measurements to identify and locate the FDI attack in PDS applications. Despite the acceptable performance of the obtained results, the predicted voltage level is not accurate due to high variations in weather situations and many uncertainties in the operation of distribution networks. A study conducted in [29] has investigated the impact of changing voltage measurements on centralized voltage regulation and control. The findings demonstrate how variations in sensor readings can impact the dynamics and reactive power injection capabilities of PV inverters. It is important to mention that low-margin coordinated attacks that may occur in PDS cannot be identified by the detection methods discussed in the previous works. In other words, the aforementioned methods in the literature have not thoroughly examined detection strategies for cyber attacks that specifically aim to manipulate the voltage regulation mechanism of PV-integrated PDSs in steady-state conditions. This is particularly important when considering the uncertainties associated with weather conditions that impact the power generation of PVs and load variations. Therefore, there is a clear need to investigate detection approaches that can effectively identify cyber attacks on voltage regulation mechanisms under these conditions.

Inspired by the above discussion and narrowing the existing research gaps, this study customizes a deep learning-based detection strategy to identify FDI attacks in the voltage control system of a PV-integrated PDS in the presence of existing uncertainties. The developed deep learning framework utilizes a Convolutional Neural Network (CNN) model, which is trained using a dataset that consists of some features, e.g., loading conditions and voltage

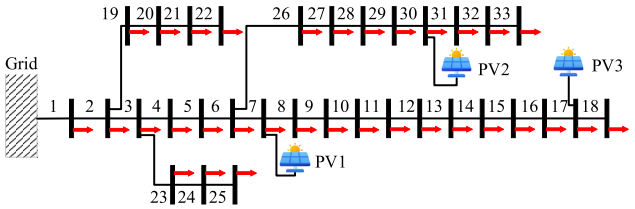

FIGURE 1. IEEE 33-bus PDS architecture.

measurements, as well as time-based factors such as season, days of the week, and holidays. During the training process, the developed CNN framework can extract practical features for classification, making this framework a proper tool for complicated applications with many uncertainties in PDS's operation compared to existing supervised and unsupervised ML-based approaches. The developed framework can also be added to the PDS operation to establish an online monitoring system based on realistic data. The performance of the developed framework is evaluated using modified IEEE 33-bus and IEEE 141-bus PDSs to demonstrate the efficiency and scalability of the customized approach. Additionally, the study demonstrates the method's noise robustness to enhance the validity and feasibility of the suggested approach in real-world scenarios. The main contribution of this paper can be listed as follows:

1) Developing a deep convolutional neural network (CNN) as a learning-based detection strategy to identify FDI attacks in the voltage control system of a PV-integrated PDS using different time-based features and measurement signals;
2) Validating the proposed detection method for frequent distribution networks and showing the acceptable performance of this method in the identification of FDI attacks compared to other machine learning approaches;
3) Adding the developed model to the PDS operation to establish an online monitoring system based on realistic data and demonstrating the feasibility of this CNN-based detection in real applications by testing the robustness of this method against noise and outlier data.

The rest of the paper is organized as follows. In Section II, both under-study power grids, i.e., IEEE 33-bus and IEEE 141-bus, including their photovoltaic systems and centralized voltage control schemes, are presented. The concept of an FDI attack and its impacts are discussed in Section III. In Section IV, the structure of the developed CNN framework is explained in detail. The simulation results and performance evaluation of the proposed methods on the IEEE 33-bus and IEEE 141-bus PDSs are presented in Section V. Finally, in Section VI, the paper is concluded and key findings are summarized.

II. MODELING OF UNDER-STUDY PDS

In this research, without loss of generality, modified versions of the IEEE 33- and 141-bus PDSs, which are obtained by adding PV panels to several of their buses, are used as the

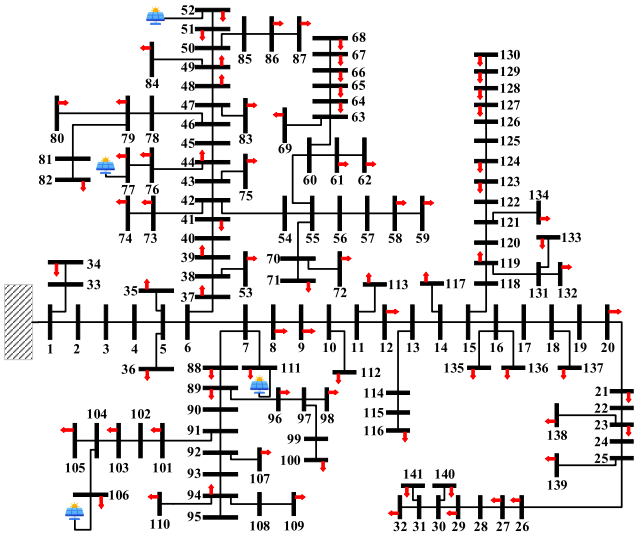

FIGURE 2. 141-bus PDS architecture.

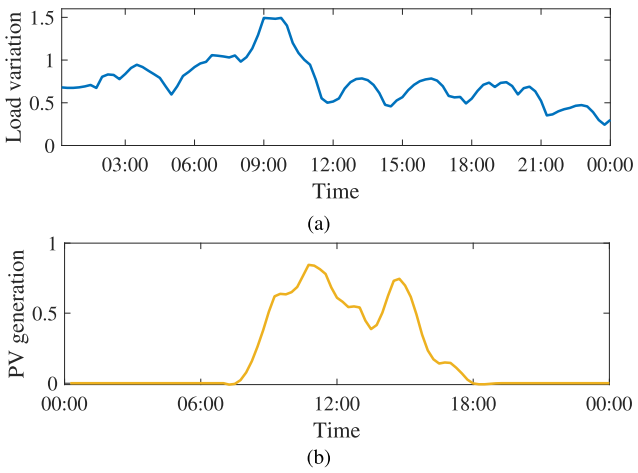

FIGURE 3. An example of (a) Load profile (b) PV generation profile in AESO dataset [30].

test system. The physical structure of IEEE 33- and 141-bus PDSs are shown in Figs. 1 and 2, respectively. In the IEEE 33-bus PDS, the nominal operating voltage is 12.66 kV, and the maximum active and reactive power components are 3.715 MW and 2.3 MVAr, respectively. The minimum voltage magnitude in the system is 0.91 per unit (p.u.) at bus 18, and the maximum voltage magnitude is 1.0 p.u. at bus 1. In this grid, the PV panels connected to buses 7, 17, and 30 [31]. Furthermore, in the IEEE 141-bus system, the total load demands were 8.2 MW and 5.1 MVAR, and the voltage magnitude changes from 0.89 p.u. at bus 52, 87 to 1.0 p.u. at bus 1. In this system, four PVs are added to buses 52, 77, 106, and 111 [32]. The acceptable voltage range within a PDS may vary based on the operator's standards. For instance, the ANSI C84.1 defines the standard for voltage variations from 0.9 p.u. to 1.05 p.u. [33] and 0.95 p.u. to 1.05 p.u. [34]. In this study, it is assumed that the desired voltage is adjusted in the

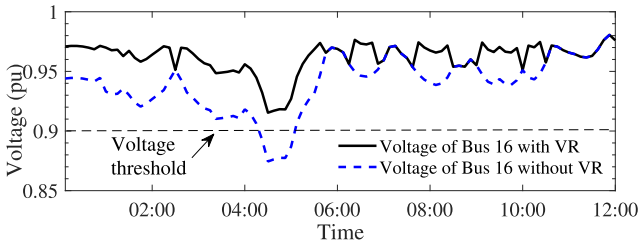

FIGURE 4. Impacts of VR scheme on the voltage profile of Bus 16.

range of 0.9 p.u. to 1.05 p.u. The operation of PV-integrated power grids must satisfy the following conditions:

- The operation of the i-th PV panel depends on its capacity constraint, which enforces that the total active (P_{PV_i}) and reactive power (Q_{PV_i}) output of the converter must not exceed a predefined value of apparent power (S_{PV_i}) [35]. It is assumed that the active power generated by each individual PV unit is 100 kW and its apparent power capacity is 500 kVA.
- The operation of i-th PV panel must comply with constraints on the voltage levels of all buses with the aim of remaining in the acceptable range of normal operation. During data generation for training the CNN model, it is assumed that changes in electricity consumption in all residential areas are similar for ordinary people. Also, solar power generation depends on the weather conditions in a specific area. On this basis, to define load profiles and PV generation capacity for IEEE 33-bus and IEEE 141-bus models, we have used the load data and photovoltaic generation data coming from past records of a regular electrical system similar to IEEE 33-bus and IEEE 141-bus systems on the website of the Alberta Electric System Operator (AESO) over a period of two years. This website can provide valuable data about load voltage profiles and wind and solar power forecasting distribution networks [30]. Fig. 3 illustrates an example of a daily load profile and PV generation.

Voltage regulation schemes—which are implemented into the distribution system control center—maintain voltage magnitudes at all the grid buses, e.g., PCC, within specified limits under varying operating conditions, such as changes in load and generation. Centralized control systems monitor and adjust the voltage levels by moderating the reactive power output of the PVs. The details of the voltage regulation scheme are explained as a pseudo-code in Algorithm 1. In addition, the details of a voltage regulation scheme for such a system in transient conditions are explained in [6]. For example, the impact of the voltage regulation using PVs on the IEEE 33-bus PDSs' voltage level is illustrated in Fig. 4. It can be observed that without injecting enough reactive power, the voltage at Bus 16 is below 0.9 p.u. limit for some periods of time. However, the voltage regulation scheme is able to bring the voltage close to its nominal value.

Algorithm 1 Voltage Regulation Algorithm

Input: Power flow data (PFD) of the system model, Acceptable voltage range (VR), Maximum reactive power limit (RPL), Time step size (TS), Analysis Window (AW)
Output: Regulated voltage value (RV)

```
Extract voltage measurements (VM) from PFD for buses with PVs and voltage regulation system;
while Simulation duration < AW do
    VM' = VM;
    while VM' not in Acceptable voltage range VR do
        Reactive power RP = 0;
        if VM' < VR_low then
            RP = RPL;
        end
        if VM' > VR_high then
            RP = −RPL;
        end
        Inject or absorb reactive power RP to regulate voltage; Check constraints such as the apparent power of the PV's converter; Run power flow to get updated VM';
    end
    Wait for TS minutes; Simulation duration = AW + TS;
end
return Regulated voltage value RV;
```

To estimate the flow of electric power in power grids, performing a power flow analysis is required. The main objective of this analysis is to determine the steady-state behavior of a system, i.e., voltages and their corresponding phase angle, which is then used to calculate the flow of power at each bus under normal operating conditions and contingency scenarios. Loads of the system are assumed to absorb current I_i when their terminal voltage is equal to V_i. Such relation can be expressed as [36]:

$$I_i = I_i^r + jI_i^i = \left(\frac{P_i + P_{PV_i} + jQ_i + Q_{PV_i}}{V_i}\right)^* \tag{1}$$

where $P_i + jQ_i$ is the power consumption of the load in complex format, $P_{PV_i} + jQ_{PV_i}$ are the power generation of the i-th PV, V_i is the voltage of the load, and I_i^r and I_i^i are the real and imaginary parts of the load currents. By applying Kirchhoff Current and Voltage laws (KVL/KCL), describing equation of the PDS can be obtained as [37]

$$\begin{pmatrix} I_{B_1} \\ I_{B_2} \\ I_{B_3} \\ . \\ . \\ . \\ I_{B_{N_b}} \end{pmatrix} = [\mathbf{BIBC}] \begin{pmatrix} I_1 \\ I_2 \\ I_3 \\ . \\ . \\ . \\ I_{N_L} \end{pmatrix} \tag{2}$$

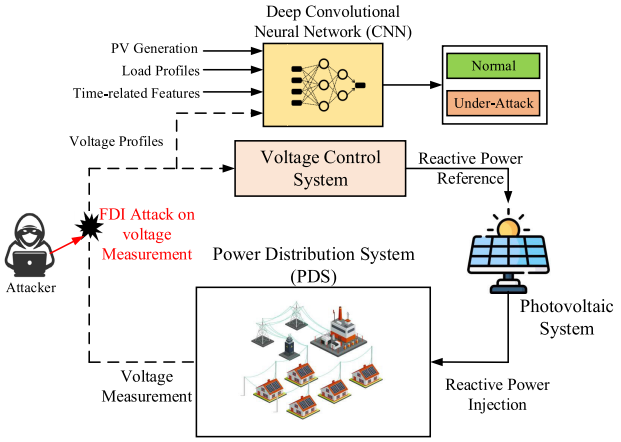

FIGURE 5. FDI attack model on the voltage regulation system of PV-tied PDS.

In this equation, the bus-injection to branch-current (**BIBC**) matrix represents the connections and topology of the distribution system; N_L is the number of loads, and N_b is the number of branches. It should be noted that this matrix depends on the topology of the system. Moreover, following the proper numbering of the system nodes, this matrix is upper triangular. The relation between the node voltages and the branch currents can also be calculated as follows [37]:

$$\begin{pmatrix} V_1 \\ V_1 \\ V_1 \\ . \\ . \\ . \\ V_1 \end{pmatrix} - \begin{pmatrix} V_2 \\ V_3 \\ V_4 \\ . \\ . \\ . \\ V_{N_L} \end{pmatrix} = [\mathbf{BCBV}] \begin{pmatrix} I_{B_1} \\ I_{B_2} \\ I_{B_3} \\ . \\ . \\ . \\ I_{B_{N_b}} \end{pmatrix} \tag{3}$$

It should be mentioned that the branch-current to bus-voltage **BCBV** matrix is also dependent on the topology of the system. Using both of these equations and load characteristics, the describing equations of the system can be written as [37]:

$$\mathbf{V} = \mathbf{V}_1 + [\mathbf{BCBV}][\mathbf{BIBC}]\mathbf{I} = \mathbf{V}_1 + [\mathbf{DLF}]\mathbf{I} \tag{4}$$

It can be observed that the matrix **DLF** is a function of the system topology. By solving the equation above, in an iterative manner, the system states can be obtained.

III. THREAT MODEL

The FDI attack on voltage profiles of a PDS is defined as the deliberate manipulation of sensor measurements to disrupt the system's voltage regulation scheme as depicted in Fig. 5. This type of attack can cause power outages and financial losses in PDSs. In order for an attack to achieve this aim, adversaries must inject false data into the voltage measurements that can result in incorrect computation of the voltage regulation controllers. This attack vector can be formulated as follows [38]:

$$z = \alpha \times \boldsymbol{V}(t) + \beta \tag{5}$$

where $\boldsymbol{V}$ is the measurement vector of PDSs, t is time, α and β are attack parameters, and z is the obtained attack vector. To design an attack, an adversary needs to obtain good values for α and β. It should be noted that the values of α and β are selected such that the attack vector does not trigger the bad data detection (BDD) algorithms of PDS.

Particle Swarm Optimization (PSO), which is a popular meta-heuristic optimization algorithm, can be used for optimizing the parameters of an FDI attack, i.e., α and β [39]. The main aim of this parameter optimization is that the measured voltage at Bus 16 in the IEEE 33-bus and Bus 52 in the 141-bus system goes below 0.9 p.u. The objective function is defined as minimizing the difference between the measured voltage and the target value of 0.9 p.u. The search space includes the possible values of α and β. The PSO algorithm is initialized by setting the number of particles (50), the maximum number of iterations (100), inertia weight (0.8), and learning factors. The fitness value is calculated for each particle in the swarm, and the particle positions and velocities are updated using the PSO equations. This process is repeated until convergence or the maximum number of iterations is reached. The optimized values of α and β are calculated as $\alpha = 1.05$ and $\beta = 0.03$. When adversaries decide to target a specific bus in the distribution network, their task involves not just launching an attack but also figuring out the right parameters tailored exclusively for the bus that they are compromising. This means they have to identify the precise settings that provide an impressive way to compromise the targeted buses. In other words, they are on a mission to discover the ideal combination to mess with that particular part of the system. On this basis, the attackers are not randomly causing trouble. They customize the attack for the chosen bus (i.e., Bus 16 in the IEEE 33-bus and Bus 52 in the 141-bus) and make the whole process more challenging.

In this study, voltage measurements are transmitted between PDS and the central controller over the IEC 60870-5-104 protocol. It is assumed that the attacker can intercept the IEC 60870-5-104 communication protocol and modify the voltage sensors between PDS and the central controller without being detected. The protocol IEC 60870-5-104 is a standard communication protocol used in electric power systems for communication between remote terminal units (RTUs) and control centers. The protocol is designed for real-time data transfer and control of electric power systems over wide-area networks. The attacker can then launch a man-in-the-middle (MITM) attack by modifying the data being transmitted between the PDS and the central controller. To execute an MITM attack on IEC 60870-5-104 protocol, the attacker can use several techniques, such as ARP spoofing, DNS spoofing, or IP spoofing, to redirect the communication channel through their device [40]. Once the communication is redirected, the attacker can modify the data being transmitted by changing the voltage measurement values based on (5).

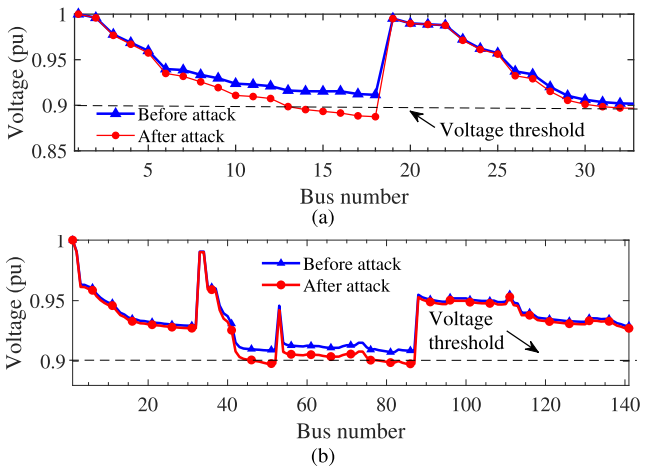

FIGURE 6. Voltage profile of (a) IEEE 33-bus and (b) 141-bus system under an FDI attack with $\alpha = 1.05$ and $\beta = 0.03$.

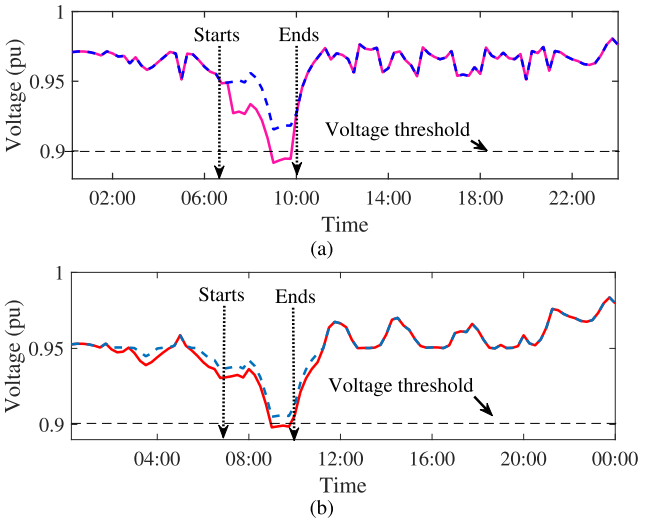

FIGURE 7. Voltage of the targeted bus in (a) IEEE 33-bus and (b) 141-bus.

The impacts of the mentioned FDI attacks on the voltage profiles of under-study power grids have been illustrated in Fig. 6 (a) and (b), respectively. It can be observed that in both systems, the voltage profiles of several buses drop below the permissible range leading to the operation of under-voltage protection systems. Furthermore, the detrimental impacts of an FDI attack on the voltage regulation of the IEEE 33-bus and 141-bus systems for 15-minute power consumption data during two years are illustrated in Fig. 7. Under normal conditions, the controller maintains voltage in acceptable ranges through proper reactive power injection and absorption. However, the FDI attack vector with parameters of $\alpha = 1.05$ and $\beta = 0.03$ can be launched from $t = 07{:}00$ a.m. to $t = 10{:}00$ a.m. leading to a significant voltage drop below the acceptable threshold due to incorrect decision of the controller. After ending the FDI attack at $t = 10{:}00$ a.m., the controller makes efforts to restore the voltage level to 0.95 p.u. to have a normal operation. It can be concluded that this type of attack can cause severe consequences on the system's operation and it is important to detect these FDI attacks on the voltage profiles in a timely manner. The following section will represent a deep learning-based algorithm for detecting this type of FDI attack in PDSs.

IV. ATTACK DETECTION FRAMEWORK

ML-based methods can be trained on a large amount of raw data to learn complex patterns for the detection of sophisticated cyber threats that can not be identified by traditional model-based approaches. Deep learning, as a supervised ML method, has been also widely deployed for attack detection in different parts of power grids. These models can be trained on a huge amount of data from power grid sensors to learn the normal behavior of the grid and detect deviations created by FDI attacks. Additionally, deep learning models can also be used to analyze historical data to identify patterns and anomalies that may indicate potential attacks in the grid. The performance of customized deep learning methods heavily depends on the adequate dataset and the structures of the learning method. In this work, a framework for attack detection in PV-integrated PDS is elaborated based on a deep CNN method to effectively detect mentioned FDI attacks on the under-study system.

A. MOTIVATION FOR USING DEEP CNN

Deep learning methods have attracted the interest of researchers in image recognition purposes. In our work, deep CNN can be also customized to detect FDI attacks in a PV-integrated PDS by transforming each row of data into a matrix similar to a set of images. This deep CNN approach can analyze high-dimensional data and make them proper for detecting FDI attacks on voltage sensor measurements. For FDI attack detection using deep CNN, first, raw data on voltage measurements and load demands are collected. Then, deep CNN extracts important features from this data and uses them to make accurate predictions about the presence of FDI attacks mentioned in the threat model. This deep learning method can be trained using a large dataset of voltage measurements, load conditions, and the amount of power generated by PVs obtained directly from the PDS during different time intervals alongside time-related properties of each sample. During the training of the model using the comprehensive dataset, any deviation from the normal operation of the under-study power grid is identified to know about the FDI attack occurrence. This helps to provide early warning of potential attacks and prevent them from causing serious damage to the power grid. Fig. 8 shows how to customize this deep learning method for the FDI attack detection in a PV-integrated PDS.

B. DATA GENERATION FOR TRAINING THE SUPERVISED CNN MODEL

In this section, the process of generating and preparing data for training a CNN model is explained. The collected data

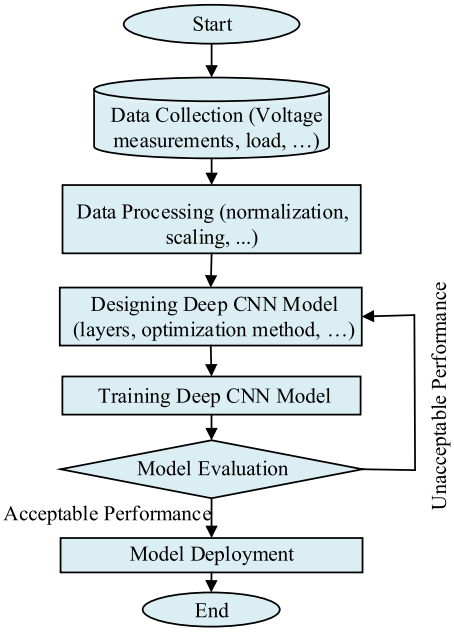

FIGURE 8. Design and implementation of a CNN method flowchart.

of the PDS should accurately represent the normal operating conditions and possible FDI attacks. While inaccurate data can lead to a biased deep learning model with poor performance, an adequate and diverse dataset can lead to a robust and comprehensive deep learning model for FDI attack detection during different conditions. Historical data from the AESO website can provide information on load conditions and photovoltaic (PV) generation, with detailed time stamps that show when each data point has been recorded. The dataset allows for the extraction of time-related features such as seasons, holidays, weekdays, and weekends, which can then be incorporated as variables during the training phase of a machine-learning model. Assimilating these time-related aspects into the model's learning process will provide the ability to discern and incorporate patterns associated with different seasons, holidays, and the distinction between weekdays and weekends. These time-related features enhance the model's capacity to make more accurate predictions and analyze load conditions and PV generation across diverse time-related contexts. To enrich the dataset for both training and testing, the obtained samples are gathered at 15-minute time intervals for two years, using the dataset described above. Since bus voltages tend to change slowly over time, a 15-minute interval can provide an adequate representation of the system's state within that period. In addition, training a model for attack detection requires a significant amount of data. Collecting data at a higher frequency may result in a much larger dataset, which can be challenging to manage and process. Moreover, 15-minute intervals are commonly used in power systems for monitoring purposes, such as SCADA systems. During each time step, the voltage regulation scheme was employed to maintain voltage profiles in the permissible range. The Algorithm 1 shows the voltage regulation system during data collection for designing a deep CNN. However, in some cases, the limitations of PV and inverter components may prevent full voltage compensation and regulation. It is important to mention that, for the IEEE 33-bus system, relevant information, e.g., bus voltages (V_1-V_{33}), load variation $\Delta P_L(0\% - 100\%)$, $P_{pv}(0\% - 100\%)$ were extracted from the power flow analysis, and then time-related features that include seasons ($S_i = \{1, 2, 3, 4\}$), and weekdays/weekends ($D_i = \{0, 1\}$) were added to the dataset. In the following, collected data is processed and converted into a proper format for the offline training of the deep CNN model. Data processing typically consists of cleaning the data, dealing with missing values, normalizing the data, scaling, and transforming the data into a compatible format. This scaling process standardizes the values across the dataset and helps to establish an efficient deep CNN model. On this basis, data can be transformed by removing the mean and scaling to unit variance. The calculation of standard scores is as follows [41]:

$$x_{new} = \frac{(x_{old} - \mu)}{\sigma} \tag{6}$$

where μ and σ are referred to as the mean and standard deviation of the training samples, respectively. This standardization process helps to ensure that the data changes around zero with the unit variance which enables a more consistent comparison of the feature values across the dataset. In this research, the *Max* normalization mode is suggested based on the infinity norm of the data. Infinity norm is a mathematical concept used to calculate the maximum absolute value of a set of numbers [42]. By using the infinity norm to normalize our data such as voltage and load conditions data, the maximum absolute value of these variables is set to 1, which can improve the convergence and performance of the proposed CNN. To prepare the data for use as input data in a CNN method, each row of data—which comprises 36 features (including 32 bus voltages, load demand levels, PV's generated power, season, and weekdays/weekends)—is reshaped into a matrix format of 12×3 matrix. It is important to mention that the bus voltage of the generator (Bus 1) is removed due to its constant value (1 p.u.), so that is why there are 32 voltage measurements in the input data. Then, the dataset is divided into training and testing sets with a common train-test ratio of 70:30.

C. DESIGNING DEEP CNN STRUCTURE

In this section, the main aim is to design a deep CNN structure considering several factors—e.g., the number of layers, the types of layers (e.g. convolutional, pooling, fully connected), activation functions, and the optimization algorithm—to be used for training of our model. This model is developed using the Sequential API of the TensorFlow library in Python. In the following, the overall steps of the customized deep CNN are described in more detail based on Fig. 9

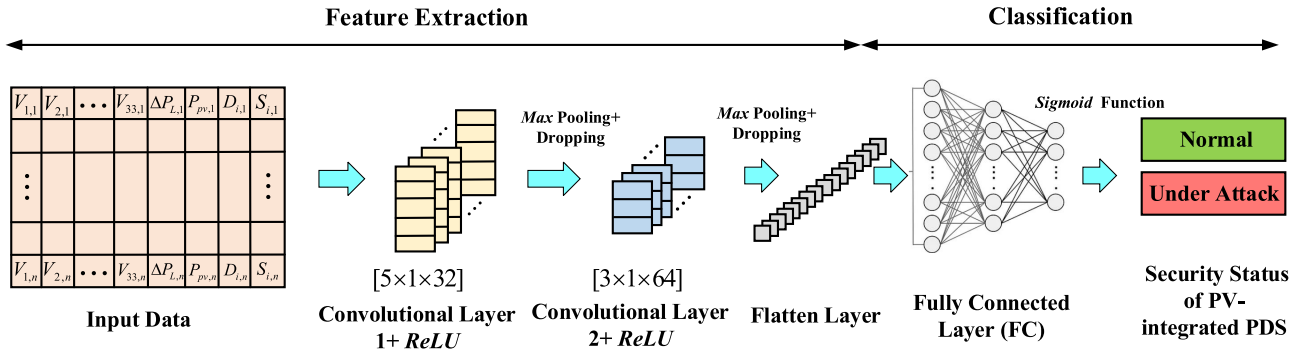

FIGURE 9. Deep CNN structure used in the developed detection framework.

- Firstly, a two-dimensional (2D) convolutional layer is applied to the processed data that helps the deep CNN model learn spatial features. To do this, 32 kernel functions of size 5×1 and the *ReLU* activation function are introduced to consider the non-linearity of input data. The 'same' padding is also applied to have the same size of output and input data.
- Then, a 2D *Maxpooling* layer is implemented with the aim of down-sampling and extracting the most important features along with the reduction in the dimension of the data. A 2×1 window is used to reduce the row dimension by a factor of 2.
- Another 2D convolutional layer with 64 kernel functions of size 3×1 is applied to learn more advanced features in the data.
- Another 2D *Maxpooling* layer to down-sample the feature maps and further reduce the dimension of under-process data.
- A dropout layer is added to set 20% of the input units to 0 randomly during the training process. This layer can prevent over-fitting by reducing the complexity of the model and forcing the remaining neurons to learn more robust features.
- A flattened layer is also added to the structure to convert the multi-dimensional output from the previous layer into a 1D vector for the next dense layer.
- After the flattened layer, a fully connected layer is also considered to introduce more non-linearity to the output and learn more complex patterns in the datasets, This fully connected layer consists of (i) a dense layer with 128 units with *ReLU* activation function and (ii) another dense layer with 64 units and the *ReLU* activation function.
- The final layer in the model is a dense layer with 1 unit and the *sigmoid* activation function. This layer produces a binary probability that indicates the predicted class. Since the output is a probability between 0 and 1, which indicates the probability that the input belongs to the positive class, the *sigmoid* activation function is used.

In the following, the deep CNN model, which has been configured by previous layers, deploys the Adam optimization algorithm [43] to update network weights through iterative gradient descent based on training data. The Adam optimization method is commonly used with the binary cross-entropy loss function in deep learning algorithms. This algorithm keeps track of the first and second moments of the gradients of the parameters and then adjusts the learning rate based on the estimated variance and mean of the gradients. This allows the algorithm to adaptively change the learning rate during training, prevent the optimization from getting stuck in local minima, and accelerate convergence. To use Adam optimization with binary cross-entropy loss, we calculate the gradient of the loss function concerning the parameters in the neural network.

Since this customized deep CNN is deployed for classification problems, a binary cross-entropy loss function L is defined to update the weights of the neural network for two classes ($i = 1$ and 2) as follows [44]:

$$\begin{aligned} L &= -\sum_{i=1}^{2} T_i \log(p_i) \\ &= -[T_1 \log(p_1) + T_2 \log(p_2)] \\ &= -[T \log(p) + (1 - T) \log(1 - p)] \end{aligned} \tag{7}$$

where T and p are the true labels and the probability of correct prediction, respectively. For a binary classification and having a set of assumptions, i.e., $T_1 = T$ $T_2 = 1 - T$, $p_1 = p$, and $p_2 = 1 - p$, the L function is simplified as [44]:

$$L = \begin{cases} -\log(p) & \text{if} \quad T = 1 \\ -\log(1 - p) & \text{if} \quad T = 0 \end{cases} \tag{8}$$

This loss function is deployed to optimize the model during training by adjusting its parameters.

D. EVALUATING CUSTOMIZED DEEP CNN

After designing a deep CNN model, its classification performance can be evaluated using several criteria, i.e., TP = True Positive, TN = True Negative, FP = False Positive, and FN = False Negative. These criteria can be obtained as follows:

TABLE 1. Trail and error for selecting hyperparameter of CNN model for IEEE 33-bus PDS.

Batch size	Learning rate	Maximum number of epoch	Accuracy (%)
10	0.005	50	89.68
10	0.004	50	89.82
20	0.004	75	90.32
20	0.003	75	90.69
25	0.002	75	90.95
25	0.002	100	91.04
25	**0.001**	**100**	**91.06**

TABLE 2. Trail and error for selecting hyperparameter of CNN model for IEEE 141-bus PDS.

Batch size	learning rate	Maximum number of epoch	Accuracy (%)
20	0.005	50	90.02
20	0.004	50	90.30
20	0.003	50	91.58
20	0.003	75	92.12
25	0.003	75	92.64
25	0.002	100	94.89
30	**0.001**	**100**	**95.30**

1) Accuracy: It is a metric to measure the percentage of correctly classified samples in the testing dataset [45]:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{9}$$

2) Confusion matrix: This matrix shows the number of true positives, true negatives, false positives, and false negatives.
3) Precision and Recall: These metrics are useful for evaluating the performance of a model when the classes are imbalanced. Precision measures the proportion of true positive predictions out of all positive predictions, while recall measures the proportion of true positives out of all actual positive samples [45]:

$$Precision = \frac{TP}{TP + FP} \tag{10a}$$

$$Recall = \frac{TP}{TP + FN} \tag{10b}$$

4) F1 score: The F1 score is a harmonic mean of precision and recall and is useful when both measures are equally important [45]:

$$F_1 score = \frac{2 \times (Precision \times Recall)}{Precision + Recall} \tag{11}$$

V. SIMULATIONS RESULTS AND DISCUSSION

In this section, the simulations are conducted on a Windows PC with a 64-bit Intel i7 core, a 2.9 GHz processor, and 16 GB RAM. Moreover, the Google Colab with Python 3.8 is also employed to run deep learning tasks and MATLAB R2020-b to collect power flow data. Firstly, the feature importance analysis is presented to determine the most important features in the dataset during the training of the proposed CNN. Then, the performance of the customized CNN is presented in a wide range of FDI attacks and compared with other ML algorithms, e.g., Random Forest (RF), K-Nearest Neighbor (KNN), Logistic Regression (LR), Support Vector Machine (SVM), and Multilayer Perceptron (MLP) for PV-integrated IEEE 33- and 141-bus PDSs. This customized machine learning method is also investigated during time domain simulations and the robustness against noise is also investigated. The values of hyperparameters for the customized CNN model for the training process, which can be obtained based on trial and error in the search space of the different hyperparameters, have been listed in Table 1 and 2. As before mentioned, the optimization algorithm is selected as Adam. The best batch size, learning rate, and maximum number of epochs are selected as 25, 0.001, and 100, for IEEE 33-bus PDS and 30, 0.001, and 100 for IEEE 33-bus PDS, respectively [46].

A. FEATURE IMPORTANCE ANALYSIS

The feature importance analysis can be carried out to understand the behavior of the dataset and identify the most effective features on the performance of the customized CNN model. In other words, the deep CNN structure can deploy the most important features during the training process with the aim of performance improvement. The input dataset for IEEE 33-bus consists of 37 columns for different operational conditions that can be listed as follows: The 1^{st} to 33^{rd} columns are voltage measurements of all buses. The next column is allocated to the load variation during the 15-minute time step. The 35^{th} column shows the amount of PV generated in the under-study system during the mentioned time step. The 36^{th} column represents a feature to show the operation of the under-study power grids during weekdays or weekends. Moreover, the 37^{th} column is added to consider the impacts of different seasons. The output dataset can be also classified into the normal operation of the PDS and under FDI attack situations. On this basis, the total features of the IEEE-33 bus can be obtained as 36. Similarly, this definition for different columns of the dataset for 141-bus is also considered to have 144 features. In Fig. 10, the feature importance analysis for the IEEE 33-bus dataset reveals that the load variation feature has a high-level score compared to other features. In contrast, the time-related feature that shows weekdays/weekends in the input dataset has the lowest importance during the detection of FDI attacks. Furthermore, Fig. 11 demonstrates that bus number 52, which is under attack and connected to PV and voltage regulation system, is the most important feature in the 141-bus system dataset and the time-related feature does not play an important role in the FDI attack detection.

The correlation between features is an essential aspect of analyzing a dataset. Figs. 12 and 13 provide a feature correlation color map for IEEE 33-bus and 141-bus systems. The color bar in both figures ranges from 1 to -1, where 1 implies two features are completely correlated, and -1 means they are reversely correlated. In Fig. 12, we observe that most voltage measurements are highly correlated with each other. However, feature number 32, the

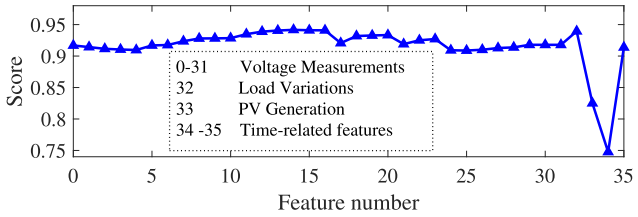

FIGURE 10. Importance of each feature in the dataset for IEEE 33-bus.

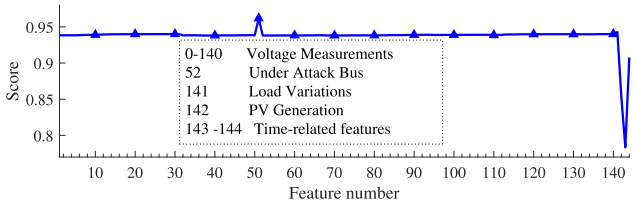

FIGURE 11. Importance of each feature in the dataset for 141-bus.

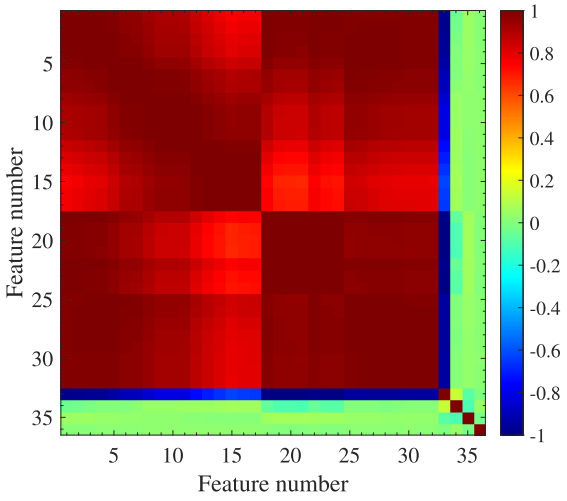

FIGURE 12. Features correlation color-map for IEEE 33-bus.

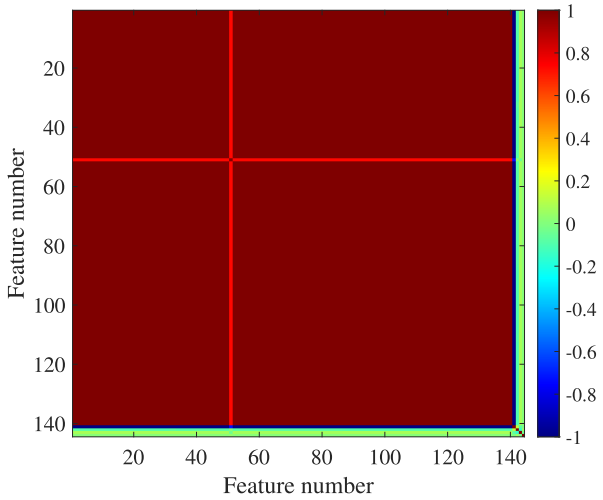

FIGURE 13. Features correlation color-map for 141-bus.

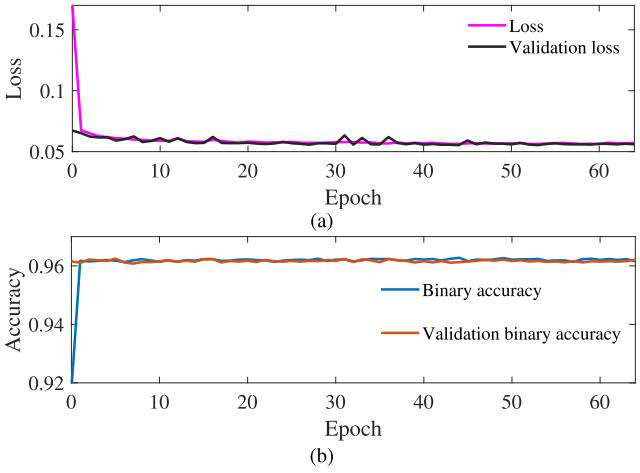

FIGURE 14. Training loss and accuracy plot for IEEE 33-bus.

load condition, is negatively correlated because an increase in load leads to a decrease in voltage. Additionally, the PV generation data and time-related features have a weak correlation with voltage measurements. Light red cells in the color map denote the under-attack bus and buses near them that have lower voltage due to the attack. Similarly, in Fig. 13, we see a similar correlation pattern. Still, feature 51, the voltage of bus 52, is lighter red, indicating that its voltage changes significantly more than other buses due to the attack.

B. PERFORMANCE OF CUSTOMIZED CNN METHOD AND ITS SCALABILITY

The training loss and accuracy plots for the IEEE 33-bus and 141-bus systems have been illustrated in Figs. 14 and 15, respectively. It can be observed from Fig. 14. (a) that the cross-entropy loss function decreases significantly in the initial epochs of training that interprets the CNN model can deliver the acceptable performance during the FDI attacks detection in the IEEE 33-bus. Furthermore, the binary accuracy during the training of this deep CNN model has been depicted in Fig. 14. (b). In Fig. 15. (a) and (b), some fluctuations in both the loss function and the accuracy can be observed for the 141-bus system during the training process due to the stochastic nature of the training algorithm. After progressing in the training phase, these fluctuations become flatter and the deep CNN model becomes more stable. Table 3 compares the detection results of our proposed CNN method for IEEE 33-bus PDS with five different ML models. The performance of the models is evaluated based on the mentioned metrics in Section IV-D, namely, accuracy, precision, recall, and F1 score. Based on the results presented in Table 3, the proposed CNN, outperforms all other ML models in terms of accuracy, precision, recall, and F1 score. The CNN achieved an accuracy of 96.24%, while the next best model, i.e., LR, achieved an accuracy of 94.50%. In terms of precision, recall, and F1 score, the CNN achieves values of 95.71%, 96.81%, and 96.26%, respectively, which

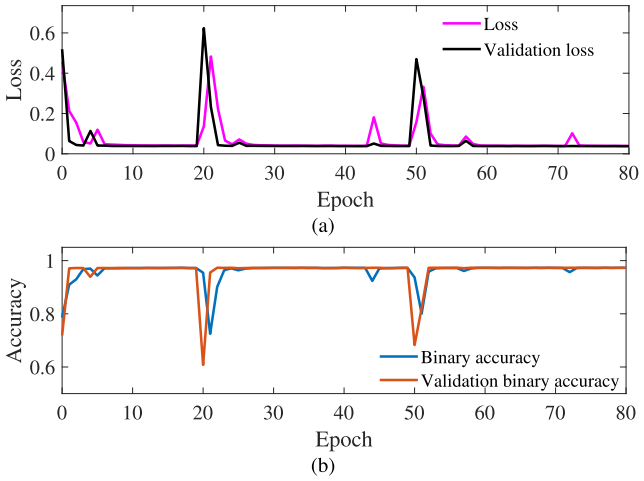

FIGURE 15. Training loss and accuracy plot for 141-bus.

TABLE 3. Detection results for IEEE 33-bus PDS.

Model \ Metric	Accuracy	Precision	Recall	F1 Score
RF	91.06	91.08	91.02	91.05
KNN	92.33	92.35	92.30	92.33
LR	94.50	95.26	93.67	94.46
SVM	94.61	94.99	94.19	94.59
MLP	94.75	92.75	97.09	94.87
Proposed CNN	96.24	95.71	96.81	96.26

are higher than those achieved by any other model. These results suggest that the CNN is highly effective in detecting attacks in the IEEE 33-bus PDS. However, some of the other models also perform well. For example, LR achieves a high accuracy of 94.50%, and SVM achieves a similarly high accuracy of 94.61%. MLP also achieves a high accuracy of 94.75% and has the highest recall of all models at 97.09%. KNN and RF, although performing slightly worse than the other models, still achieve relatively high accuracy of 92.33% and 91.06%, respectively.

The results in Table 4 show the efficiency and scalability of our proposed CNN method in detecting attacks in the 141-bus PDS. The CNN achieved the highest F1 score of 97.36%, which is significantly higher than all the other models. LR, SVM, and MLP achieved F1 scores of 95.53%, 96.92%, and 96.82%, respectively, which were lower than CNN's F1 score. KNN and RF achieved even lower F1 scores of 93.90% and 95.30%, respectively, which were more than 1% lower than CNN's F1 score. The CNN also achieved high precision and recall values, indicating that it was able to detect attacks with high accuracy while minimizing false alarms. The results of the 141-bus PDS test also demonstrate the scalability of our CNN method, as it can achieve high detection accuracy on a larger and more complex power system than the IEEE 33-bus PDS. This is particularly important because real-world PDSs are often large and complex. In summary, the proposed method showed better performance on the 141-bus system than the IEEE 33-bus since the 141-bus PDS has more buses

TABLE 4. Detection results for 141-bus PDS.

Model \ Metric	Accuracy	Precision	Recall	F1 Score
RF	95.30	95.28	95.31	95.30
KNN	93.90	93.94	93.86	93.90
LR	95.71	99.70	91.69	95.53
SVM	97.01	1.0	94.03	96.92
MLP	96.92	1.0	93.85	96.82
Proposed CNN	97.31	95.41	99.40	97.36

and branches than the IEEE 33-bus system, which means there is more data available for training and testing ML models. With more data, ML algorithms can learn more complex patterns and relationships between the features, making it easier to detect anomalies and attacks.

C. DESIGNING A REAL-TIME MONITORING SYSTEM USING DEEP CNN

The outcome of the proposed method in the real-time domain is illustrated in Fig. 16. The method detects the red area as an attack, while the green area represents a normal operation. As can be observed, the developed model can successfully identify the attack; however, since the performance of the controller is not considered in the training, the CNN also identifies the controller's reaction to the attack as a problem. From this perspective, the role of the controller will be considered in the next step. The VR system in certain buses equipped with PV systems receives feedback from another bus (not PCC) and then adjusts the voltage of that bus instead of regulating its bus. For instance, in the IEEE 33-bus PDS, the PV system installed in Bus 7 and 17 would attempt to regulate the voltage of Bus 18, which has the lowest voltage among all the buses, or Bus 30 would try to regulate the voltage of Bus 33. In this strategy, the PV should also ensure that its voltage does not exceed the specified range. This type of regulation strategy can be used to address voltage instability issues in PDS and maintain the voltage within an acceptable range. In this scenario, the attacker intercepts the communication, receives the voltage measurement of Bus 18, and maliciously changes the voltage measurement according to the (5). According to the results summarized in Table. 5, the CNN-based attack detection method performs better than the alternative scenario when the PVs try to regulate PCC voltage. This is attributed to the fact that Bus 18 has a higher likelihood of exceeding the acceptable voltage range because its voltage is comparatively lower than the other buses in the system. In summary, based on Fig. 5, a set of data related to the voltage of different buses, load profiles, PV power generations, and time-related features, e.g., seasons, weekdays, and weekends, can go through the trained CNN detection system. The output of this CNN model provides information about the situation of the system, i.e., attack or normal conditions. It is assumed that these input data can be measured and updated every second. As a result, it will take about one second to correctly detect attacks

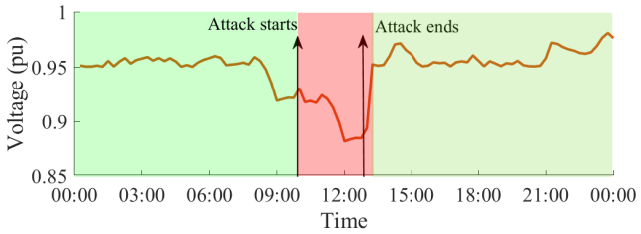

FIGURE 16. Results of the proposed method for attack detection during a day.

TABLE 5. Detection results in IEEE 33-bus PDS when the PV regulates the voltage of other buses.

Model \ Metric	Accuracy	Precision	Recall	F1 Score
RF	92.06	92.46	92.31	92.38
KNN	94.83	94.87	94.77	94.81
LR	96.33	97.15	95.90	96.52
SVM	96.94	97.35	96.82	97.08
MLP	97.84	97.46	98.15	97.80
Proposed CNN	99.91	99.92	99.90	99.91

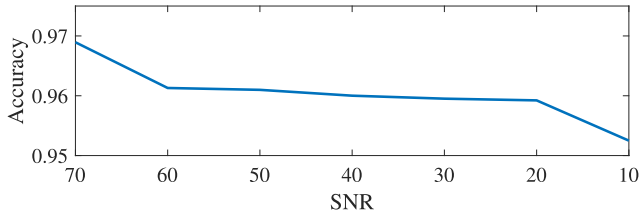

FIGURE 17. Noise robustness of the proposed method for IEEE 33-bus.

consecutively, making this trained CNN model an online detection framework for distribution system operators.

D. VERIFYING THE ROBUSTNESS OF THE PROPOSED METHOD AGAINST NOISE

In a PDS, the transmitted data can be susceptible to noise, and this can lead to difficulties in the accurate detection of attacks. To address this issue, it is important to use a detection method that is robust to noise. The developed detection method ensures that the system can reliably detect attacks in real-world scenarios in the presence of noise. Figure. 17 demonstrates the accuracy of our detection method when the signal-to-noise ratio (SNR) varies between 10 to 70. The collected results show that the accuracy does not change significantly in the presence of noise. However, when the SNR is reduced, the accuracy may decrease slightly.

VI. CONCLUSION

This paper proposed a data-driven framework based on a CNN model for identifying FDI attacks against voltage regulation of PV-integrated PDSs. The proposed CNN framework was trained on a realistic dataset that covered all normal conditions and unpredictable changes in a PDS. According to the obtained results, it can be concluded that the proposed CNN delivered a more acceptable performance compared to the mentioned ML models in terms of accuracy, precision, recall, and F1 score. This model achieved an accuracy of 96.24%, while the next best model, i.e., LR, achieved an accuracy of 94.50%. In terms of precision, recall, and F1 score, the CNN achieves values of 95.71%, 96.81%, and 96.26%, respectively, which are higher than those achieved by any other model. The scalability of the proposed method was also demonstrated by testing it on a larger PDS with 141 buses. In this situation, the proposed CNN model also achieved the highest F1 score of 97.36%, which was significantly higher than all the other models. Although LR, SVM, and MLP achieved F1 scores of 95.53%, 96.92%, and 96.82%, respectively, their performance was lower than CNN's F1 score. Moreover, the KNN and RF achieved even lower F1 scores of 93.90% and 95.30%, respectively, which were more than 1% lower than CNN's F1 score. The proposed framework has provided an effective monitoring tool for protecting PDSs against cyber threats and ensuring the secure and reliable operation of power systems. The convolutional layers in the CNN can identify spatial correlations within the input data and extract important features using the fully connected layers to make an accurate classification decision. The ability of the developed CNN model to automatically learn relevant features from raw input data, combined with its scalability, noise robustness, and high accuracy, make it a promising method for real-world applications in power system security. In the future, we are going to develop this deep CNN learning model for other types of attacks on the control framework during voltage regulations.

REFERENCES

[1] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. A. Jiménez-Estévez, and N. D. Hatziargyriou, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, Jul. 2014.

[2] S. Datta, A. Baul, G. C. Sarker, P. K. Sadhu, and D. R. Hodges, "A comprehensive review of the application of machine learning in fabrication and implementation of photovoltaic systems," *IEEE Access*, vol. 11, pp. 77750–77778, 2023.

[3] J. Wu, F. Wu, K. Lin, Z. Wang, L. Shi, and Y. Li, "An improved AP clustering algorithm based critical nodes identification for distribution network with high PV penetration," *IEEE Access*, vol. 10, pp. 124619–124628, 2022.

[4] G. C. Pyo, H. W. Kang, and S. I. Moon, "A new operation method for grid-connected PV system considering voltage regulation in distribution system," in *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–7.

[5] C. Dai and Y. Baghzouz, "On the voltage profile of distribution feeders with distributed generation," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jan. 2003, pp. 1136–1140.

[6] M. Ahmadzadeh, A. Abazari, and M. Ghafouri, "Detection of FDI attacks on voltage regulation of PV-integrated distribution grids using machine learning methods," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Dec. 2022, pp. 73–78.

[7] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, Jul. 2016.

[8] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495–500.

[9] A. Abazari, M. Ghafouri, R. Atallah, and C. Assi, "Detection and mitigation methods of attacks on low-inertia hybrid microgrids: A short survey," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Dec. 2022, pp. 85–90.

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[11] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 2, pp. 101–107, Jun. 2019.

[12] H. Guo, J. Sun, and Z.-H. Pang, "Stealthy FDI attacks against networked control systems using two filters with an arbitrary gain," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 7, pp. 3219–3223, Jul. 2022.

[13] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2019, pp. 108–112.

[14] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101994.

[15] P. L. Bhattar, N. M. Pindoriya, and A. Sharma, "A combined survey on distribution system state estimation and false data injection in cyber-physical power distribution networks," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 6, no. 2, pp. 41–62, Jun. 2021.

[16] M. Fotopoulou, S. Petridis, I. Karachalios, and D. Rakopoulos, "A review on distribution system state estimation algorithms," *Appl. Sci.*, vol. 12, no. 21, p. 11073, Nov. 2022.

[17] Y. Liu, O. Ardakanian, I. Nikolaidis, and H. Liang, "False data injection attacks on smart grid voltage regulation with stochastic communication model," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 7122–7132, May 2023.

[18] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures," in *Proc. Amer. Control Conf.*, Jun. 2014, pp. 4372–4378.

[19] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016.

[20] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *J. Mod. Power Syst. Clean Energy*, vol. 8, no. 4, pp. 669–678, Jul. 2020.

[21] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, no. 5, p. 1380, Mar. 2021.

[22] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[23] Y. Wu, S. Zhao, Z. Xing, Z. Wei, Y. Li, and Y. Li, "Detection of foreign objects intrusion into transmission lines using diverse generation model," *IEEE Trans. Power Del.*, vol. 38, no. 5, pp. 3551–3560, 2023.

[24] Z. Xing, S. Zhao, W. Guo, F. Meng, X. Guo, S. Wang, and H. He, "Coal resources under carbon peak: Segmentation of massive laser point clouds for coal mining in underground dusty environments using integrated graph deep learning model," *Energy*, vol. 285, Dec. 2023, Art. no. 128771.

[25] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[26] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, Oct. 2020.

[27] Q. Li, J. Zhang, J. Zhao, J. Ye, W. Song, and F. Li, "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2369–2380, May 2022.

[28] N. Bhusal, M. Gautam, and M. Benidris, "Detection of cyber attacks on voltage regulation in distribution systems using machine learning," *IEEE Access*, vol. 9, pp. 40402–40416, 2021.

[29] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, "Cyber security risk assessment of solar PV units with reactive power capability," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2018, pp. 2872–2877.

[30] *Data Requests*. Accessed: 2023. [Online]. Available: https://www.aeso.ca/market/market-and-system-reporting/

[31] L. Luo, W. Gu, Y. Wang, and C. Chen, "An affine arithmetic-based power flow algorithm considering the regional control of unscheduled power fluctuation," *Energies*, vol. 10, no. 11, p. 1794, Nov. 2017.

[32] T. Gangwar, N. P. Padhy, and P. Jena, "Storage allocation in active distribution networks considering life cycle and uncertainty," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 339–350, Jan. 2023.

[33] *ANSI C84.1 Electric Power Systems and Equipment—Voltage Ranges*. [Online]. Available: http://www.powerqualityworld.com/2011/04/ansi-c84-1-voltage-ratings-60-hertz.html

[34] A. Joseph, K. Smedley, and S. Mehraeen, "Secure power distribution against reactive power control malfunction in DER units," *IEEE Trans. Power Del.*, vol. 36, no. 3, pp. 1552–1561, Jun. 2021.

[35] Y.-B. Wang, C.-S. Wu, H. Liao, and H.-H. Xu, "Steady-state model and power flow analysis of grid-connected photovoltaic power system," in *Proc. IEEE Int. Conf. Ind. Technol.*, Apr. 2008, pp. 1–6.

[36] R. Roshan, B. S. Ravishankar, N. Mohan, K. J. S. Kumar, and D. G. Devaru, "Reassessment of power losses and enhancement of techno-economic feasibility in a radial distribution system," in *Proc. IEEE 2nd Mysore Sub Sect. Int. Conf. (MysuruCon)*, Oct. 2022, pp. 1–6.

[37] T. Thakur and J. Dhiman, "A new approach to load flow solutions for radial distribution system," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo., Latin Amer.*, May 2006, pp. 1–6.

[38] Md. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 3153–3158.

[39] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proc. Int. Conf. Neural Netw. (ICNN)*, vol. 4, Aug. 1995, pp. 1942–1948.

[40] P. Maynard, K. Mclaughlin, and B. Haberler, "Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks," in *Proc. 2nd Int. Symp. ICS & SCADA Cyber Secur. Res.*, 2014, pp. 30–42.

[41] *Sklearn.Preprocessing.Standardscaler*. Accessed: 2023. [Online]. Available: https://scikit-learn.org/stable/modules/preprocessing.html

[42] G. Strang, *Linear Algebra and Its Applications* Belmont, CA, USA: Thomson, Brooks/Cole, 2006.

[43] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.

[44] Y. Ho and S. Wookey, "The real-world-weight cross-entropy loss function: Modeling the costs of mislabeling," *IEEE Access*, vol. 8, pp. 4806–4813, 2020.

[45] M. Elimam, Y. J. Isbeih, S. K. Azman, M. S. E. Moursi, and K. A. Hosani, "Deep learning-based PMU cyber security scheme against data manipulation attacks with WADC application," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2148–2161, May 2023.

[46] Y. Du, F. Li, J. Li, and T. Zheng, "Achieving 100× acceleration for N-1 contingency screening with uncertain scenarios using deep convolutional neural network," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3303–3305, Jul. 2019.

MASOUD AHMADZADEH received the B.Sc. degree from Amirkabir University, in 2020, and the M.Sc. degree from Concordia University, in 2023. His research interests include cyber security and the application of machine learning in power systems.

AHMADREZA ABAZARI (Member, IEEE) received the B.Sc. degree in electrical engineering from the Sharif University of Technology, in 2013, and the M.Sc. degree in power system engineering from the University of Tehran, the most highly prestigious university in Iran, in 2016. He is currently pursuing the Ph.D. degree with the Security Research Center, Concordia University, Montreal, QC, Canada. He is also a Researcher with Institut de recherche en électricité du Québec (IREQ), QC. He has authored or coauthored 18 publications in top-ranked journals, including IEEE, Elsevier, and IET, and IEEE international conferences. He has reviewed many papers in prestigious journals, e.g., IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL CYBER-PHYSICAL SYSTEMS, IEEE ACCESS, *IET Generation*, *Transmission and Distribution*, *IET Renewable, Power, and Generation*, *Electric Power System Research* (EPSR), and *Electrical Engineering* (Springer). His research interests include the dynamic stability of power systems, the control of AC/DC microgrids, cyber security in smart grids, and the applications of machine learning and data-mining methods in modern power systems.

MOHSEN GHAFOURI (Member, IEEE) received the B.Sc. and master's degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2009 and 2011, respectively, and the Ph.D. degree in electrical engineering from Polytechnique Montréal, Montreal, QC, Canada, in 2018. He was a Researcher with the Iranian Power System Research Institute, Sharif University of Technology, from 2011 to 2014. In 2018, he was a Researcher with CYME International, Eaton Power System Solutions, Montreal. In August 2018, he joined the Security Research Group, Concordia University, as the Horizon Postdoctoral Fellow, where he is currently an Assistant Professor. His research interests include the cybersecurity of smart grids, power system modeling, microgrid, wind energy, and the control of industrial processes.

AMIR AMELI (Member, IEEE) received the B.Sc. degree in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2011, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, in 2013, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 2019. He was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, from August 2019 to July 2020. He is currently an Assistant Professor with the Department of Electrical Engineering, Lakehead University, Thunder Bay, ON, Canada. His current research interests include power systems cyber-security and protection.

S. M. MUYEEN (Fellow, IEEE) received the B.Sc. degree in electrical and electronic engineering from the Rajshahi University of Engineering and Technology (RUET, formerly known as the Rajshahi Institute of Technology), Bangladesh, in 2000, and the M.Eng. and Ph.D. degrees in electrical and electronic engineering from the Kitami Institute of Technology, Japan, in 2005 and 2008, respectively. He is currently a Full Professor with the Department of Electrical Engineering, Qatar University. He has published more than 250 papers in different journals and international conferences. He has also published seven books as the author or an editor. His research interests include power system stability and control, electrical machine, FACTS, energy storage systems (ESSs), renewable energy, and HVDC systems. He is a fellow of Engineers Australia. He is serving as an Editor/Associate Editor for many prestigious journals, such as IEEE, IET, and other publishers, including IEEE TRANSACTIONS ON ENERGY CONVERSION, IEEE POWER ENGINEERING LETTERS, *IET Renewable Power Generation*, and *IET Generation, Transmission and Distribution*. He has been a keynote speaker and an invited speaker at many international conferences, workshops, and universities.

Open Access funding provided by 'Qatar National Library' within the CRUI CARE Agreement