SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V13I11P105

Volume 13 Issue 11, 69-88, November 2026
© 2026 Seventh Sense Research Group®

Original Article

Gated Recurrent Unit based Detection of False Data Injection and Denial of Service Attacks in Standalone PV Powered EV Charging System

G. Sangeetha[1], D. Suchitra[2]

[1,2]*Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.*

[1]*Corresponding Author: sangeethaphd2109@gmail.com*

Received: 22 August 2026 Revised: 22 October 2026 Accepted: 31 October 2026 Published: 25 November 2026

Abstract - *The rapid deployment of renewable energy powered electric vehicle charging infrastructure has intensified the demand for intelligent cybersecurity mechanisms capable of sustaining uninterrupted charging operations under hostile conditions. Standalone photovoltaic powered Electric Vehicle Charging Stations (EVCS) which lack grid backup and centralized monitoring are inherently vulnerable to cyber physical attacks that can disrupt charging services and jeopardize system safety. This paper presents a Gated Recurrent Unit (GRU) based anomaly detection framework to identify cyber physical anomalies in standalone EVCS with high reliability. The proposed attack model incorporates both false data injection and denial of service attacks by altering sensor measurements and disrupting the converter control strategy of the EVCS. A comprehensive MATLAB/Simulink EVCS model is implemented on an OPAL-RT real-time simulator to evaluate system behaviour during attacks, while the detection method is trained and evaluated offline using the logged data. Time series electrical measurements and converter control signals from the EVCS are gathered under both normal operating settings and cyber-physical attack scenarios to enable system behaviour analysis. The proposed GRU-based detector obtains an accuracy of 99.91 ± 0.03%, a macro precision of 99.95 ± 0.05%, a macro recall of 99.73 ± 0.06%, and a macro F1-score of 99.84 ± 0.05% across five separate training sessions with leakage free train, validation and test splits. The proposed GRU method outperforms the LSTM, Bi-LSTM, CNN-LSTM and CNN-GRU benchmark models in terms of accuracy and macro F1-score while requiring only 26,691 trainable parameters, demonstrating high detection performance with compact model architecture for standalone electric vehicle charging systems.*

Keywords - *Electric Vehicle Charging Stations (EVCS), Cyber physical systems, Cybersecurity, Artificial intelligence, Anomaly detection.*

1. Introduction

The expansion of electric mobility relies on a robust infrastructure for charging electric vehicles that can provide dependable and accessible charging services by combining sophisticated grid technologies, communication networks, power converters, charging stations and renewable energy sources [1]. The rising digitization of EVCS through next generation communication networks, internet of things and AI-driven control techniques has increased operational intelligence while also expanding the attack surface, exposing EVCS to a variety of cyber physical vulnerabilities [2-5]. Cyber physical attacks are classified into two types: physically induced cyberattacks, which target physical components such as controllers and embedded devices and cyber induced physical attacks, which exploit vulnerabilities in communication and control infrastructure through FDI, man in the middle and DoS attacks [6, 7]. Artificial intelligence and machine learning algorithms enable proactive cyber threat identification by continuously monitoring system data and identifying unusual trends. Their capacity for adaptive learning provides safe, reliable and continuous charging services while strengthening EVCS's resilience [8].

Despite these advancements, standalone PV powered EVCS pose significant cybersecurity challenges due to a lack of utility grid support and centralized monitoring. Backup power routes, grid level protection relays and centralized SCADA oversight in grid connected and microgrid integrated EVCS enable a compromised charging station to be separated or supported by an alternate source while an anomaly is examined. Unlike grid connected or microgrid integrated EVCS, standalone EVCS rely on local PV generation, battery energy storage and converter controls, which leaves limited scope for independent verification or backup during attacks. As a result, FDI and DoS assaults can directly affect local measurements and charging operations, emphasizing the requirement for dedicated real time cyber


This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

physical anomaly detection in standalone EVCS. Existing research on cyber physical anomaly detection in Electric Vehicle Charging Stations (EVCS) has mostly focused on grid connected and microgrid integrated systems, as detailed in Section 2.

Most research focuses on false data injection or denial of service attacks, which necessitate different detection systems for sensor data manipulation and service disruption. Reliable local detection is especially crucial in standalone EVCS when grid support and centralized monitoring are unavailable. However, the multiclass detection of normal operation, FDI attacks on the sensor path, and DoS attacks on the actuation path, with the attacks occurring independently at various time instants, has received little attention in standalone EVCS. Additionally, while EVCSs and related power-electronic systems have investigated recurrent, convolutional, attention based, and autoencoder based detectors [11, 12, 15, 21-24], their performance has often been assessed using system-specific datasets and experimental methodologies. The use of real-time simulation to reproduce the attack induced responses in the charging mechanism also remains underexplored. These shortcomings highlight a research gap in the development and assessment of a multiclass detector of independent FDI and DoS assaults for standalone PV powered EVCS.

Unlike the hidden Markov model and forecasting error based FDI detection techniques in [9, 10] the proposed approach uses the standalone EVCS's intrinsic electrical signatures instead of grid referenced data. The proposed method detects the physical impact of DoS/DDoS assaults on the charging system, which is represented by the forced reduction of the buck converter duty cycle, while the DoS/DDoS detection techniques in [13-16] mostly describe attacks through communication or network traffic. This enables detection without relying on network layer telemetry.

Furthermore, unlike the deep learning methods in [18-24] and the Bi-LSTM based detector in [12], which focus on grid connected, microgrid integrated systems and network traffic. The proposed framework models both an FDI attack and a DoS attack on the same standalone EVCS and classifies them using a multiclass GRU and reproduces the attack responses on an OPAL-RT real time simulator. The novelty of this work lies in integrating the standalone EVCS modelling, independent FDI and DoS attack modelling scenarios, multiclass attack detection using electrical and control features and real time simulation for assessing the attack induced response of the EVCS. The core contributions of the proposed work are outlined below.

- The proposed attack modelling approach is developed to investigate two independent FDI and DoS cyberattacks targeting the EV charging subsystem of a standalone EVCS. These attacks are introduced at different locations and time instants to assess their impacts on the station's electrical response.
- A compact two-layer GRU detector is developed for multiclass attack (normal, FDI and DoS) classification from electrical and control signal measurements. Its performance is benchmarked against various models, including LSTM, Bi-LSTM, CNN-LSTM, CNN-GRU, attention-based GRU and a hybrid autoencoder under a common leakage free evaluation protocol.
- The proposed detector is evaluated through hyperparameter sensitivity, ablation studies and robustness analyses under varying operating conditions to assess its potential for real time attack detection.

The following sections of the paper are outlined as follows: Section 2 surveys the existing literature on cyber physical anomaly detection in EVCS and highlights the research gap that motivates this work. Section 3 details the architectural layout of the cyber physical standalone PV powered EVCS system. Section 4 introduces the proposed cyberattack modelling framework developed for the EVCS. Section 5 explains the gated recurrent unit-based anomaly detection methodology for detecting cyberattacks. Section 6 provides the results along with their discussions. Finally, Section 7 synthesizes the key research findings and highlights opportunities for future research.

2. Literature Review

Existing research works on cyber physical anomaly detection in EVCS can be divided into three categories: false data injection attack detection, denial of service attack detection and deep learning and reinforcement learning based intrusion detection methods. This section examines typical studies in these domains and identifies the limits of existing techniques with a focus on the research gap in standalone PV powered EVCS system. Several studies have investigated FDI attack detection in grid connected and microgrid integrated EVCS environments. A weighted attack defence tree technique was utilised to predict attack scenarios, and a hidden Markov model was developed to identify false data injection attacks in cyber physical fast charging infrastructure, but this approach was restricted to grid metrics [9]. False data injection attack was detected in EVCS data marketplaces using a forecasting error monitoring technique within vehicle to grid enabled microgrids [10]. A hybrid convolutional neural network and autoencoder architecture was employed to capture charge manipulation attacks that occurred during smart charging intervals in the grid connected EVCS [11].

A Bi-LSTM based anomaly detection framework was introduced to detect data manipulation attacks and FDI attacks, and it was tested on a DER-integrated microgrid model [12]. A separate line of investigation has concentrated on DoS and DDoS assaults. A decision tree based machine learning classifier was utilised to detect DoS attacks at the cyber-physical layer in fast EVCS considering bidirectional

operations in microgrids [13]. In an EVCS coupled with the IEEE 33-bus distribution test system, denial of service attack was detected using a time-varying Poisson process [14]. LSTM and feed forward neural network models were employed to detect DDoS assaults in EVCS communication networks using the CICEV2023 dataset [15]. A hybrid VGG19 deep neural network linked with the Harris Hawks optimization algorithm was used to detect DDoS attacks in EVCS communication networks [16]. Deep learning and reinforcement learning methods have recently been investigated for identifying abnormal behaviour in cyber physical systems. Reinforcement learning was applied to synthesize adversarial attacks, and a feedforward neural network was leveraged to detect these adversarial threats against charging coordination systems [17]. Intrusion detection approaches were framed for identifying cyberattacks in IoT-enabled EVCS. The IoT-23 dataset was used to validate the performance of several classification approaches for detecting attacks in IoT based EVCS systems [18]. A denial of charging assault was modelled and experimentally proven in an EVCS, altering normal charging operations and causing operational inefficiencies [19]. A multi-agent deep reinforcement learning framework was developed to identify FDI attacks and communication delays that damaged EV charging station communication infrastructure [20]. In order to identify irregularities in charging and power-electronic systems, recent research has also analysed deep learning architectures. In order to identify anomalous traffic in vehicle charging and station power supply systems, a multi-head attention model based on the Transformer encoder was proposed. It was tested on two power industrial control testbeds, one of which contained a charging station, and it captured correlations in industrial control traffic that traditional traffic-based detectors miss [21]. In comparison to the local outlier factor detectors, a ResNet autoencoder framework that integrates cyber and physical anomaly detection was trained without labels on controller area network data from an EV charging testbed, and it produced high accuracy and the shortest training and inference times among the neural baselines [22]. A Transformer-based detector trained using secure federated learning was compared with CNN and LSTM detectors under various measurement noise levels for FDI attacks on power system measurements [23]. An artificial neural network and model predictive control were used in DC microgrids to identify and eliminate FDI attacks on converter level signals [24]. Table 1 presents a comparative overview of existing anomaly detection methods for EV charging systems.

Table 1. Comparative overview of existing anomaly detection methods for Electric Vehicle Charging Stations (EVCS)

Ref	Technique/Model Used	Attacks	System Used	Accuracy level	Remarks
[9]	Hidden Markov Model	FDI	Grid tied	Not Reported	Focused only on grid related metrics
[10]	Game theoretic modelling and Forecasting error monitoring method	FDI	V2G enabled Microgrid	Not Reported	No explicit detection or evaluation metrics
[11]	Unsupervised Auto encoder Model	Data manipulation	Grid connected	91.24%	Unsupervised model lacks multiclass detection
[12]	Bidirectional Long Short-Term Memory	FDI/Data manipulation	Microgrid (DER-integrated EVCS)	99.42%	Limited to microgrid systems
[13]	Decision Tree Classifier Model	DoS	V2G enabled Microgrid	Not Reported	Weak temporal attack modelling
[14]	Time variant poisson process modelling	DDoS	Smart grid	Not Applicable	Focused on attack modelling and no detection metrics
[16]	Hybrid VGG19 DNN and Harris Hawks Optimization Algorithm	DDoS	Smart Grid	99.82%	Focused attacks on communication layer only
[17]	Reinforcement Learning Model	SoC falsification	Microgrid	Not Reported	No optimization for precision/recall
[20]	Multi Agent Deep Reinforcement Learning	Replay	Grid integrated systems	Not Reported	Focused on resilience strategy

3. Cyber Physical Architecture of Standalone PV Powered EVCS

The EVCS is designed as a standalone, off-grid infrastructure powered by photovoltaic energy that incorporates three integral electrical subsystems: the PV generation subsystem, the energy storage subsystem and the EV charging subsystem. The block diagram displayed in Figure 1 depicts the overall configuration and connections of these modules. The PV generation subsystem consists of a photovoltaic array, a boost converter, a maximum power point tracking controller, and a pulse width modulation generator.

The key electrical parameters of the photovoltaic array are represented by a single diode equivalent circuit as formulated by the characteristic equation below in Equation (1) [25].

$$I = I_{phs} - I_{ds}.\left\{e^{\frac{q}{N.k.Temp.\gamma}.(V_p + I_p.R_{Se})} - 1\right\} - \frac{V_p + I_p.R_{Se}}{R_{Sht}} \quad (1)$$

Where V_p and I_p are the voltage and current of the photovoltaic module, and N, Temp, q and k represent the number of cells, temperature of the cell, elementary charge and Boltzmann constant. Model parameters include series resistance R_{Se}, shunt resistance R_{sht}, saturation current of the diode I_{ds}, ideality factor of the diode γ and photocurrent I_{phs},.

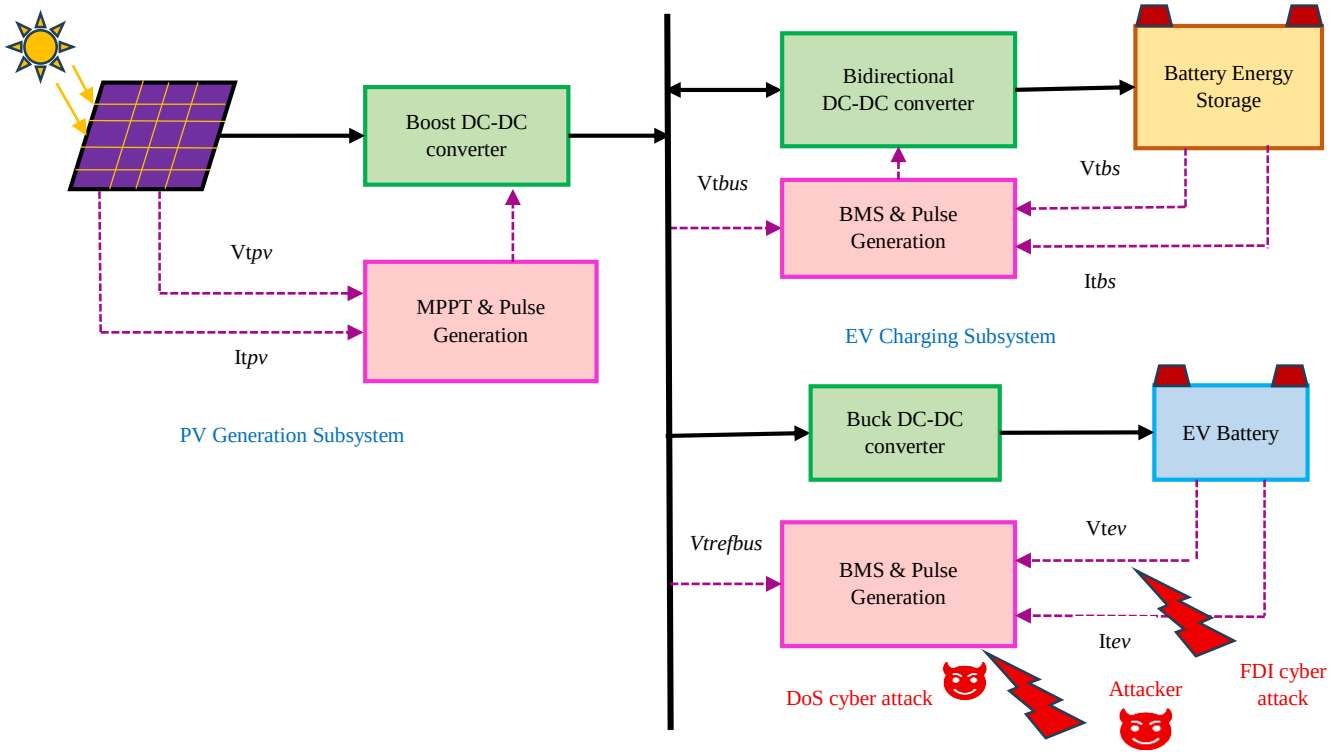


Fig. 1 Cyber physical system architecture of standalone PV powered EVCS

The MPPT controller receives the continuously monitored photovoltaic output voltage Vt_{pv} and current It_{pv} as its input signals. Using the Perturb and Observe (P&O) algorithm, the controller determines the operating range corresponding to maximum power extraction and changes the duty cycle accordingly, generating the required boost switching signal through the PWM generator. The P&O MPPT algorithm is described in [26]. The boost converter, which operates on a PWM duty cycle, increases the photovoltaic output voltage to the desired DC bus level, providing maximum power extraction under varied operating conditions. The boost converter's inductor (L) and capacitor (C) parameters are determined using the design formulae presented in [26].

The energy storage subsystem consists of a Battery Energy Storage (BES), a bidirectional DC-DC converter, and a control mechanism that regulates energy exchange with the DC bus. The converter's operating mode varies dynamically in response to the power balance of the PV-powered EVCS. Under excess PV generation, it acts as a buck type converter transferring energy from the DC bus to the BES. During periods of low PV availability, it functions in boost mode, delivering stored battery energy to the DC bus while maintaining the necessary bus voltage for EV charging.

The BES controller generates PWM gating signals that drive the Bidirectional DC-DC Converter (BDC), allowing for a smooth transition between charging and discharging modes. Within a freestanding EVCS, the battery energy storage system plays an important role in ensuring continuous power supply during periods of restricted or unavailable renewable generation. The BES controller continuously senses the It_{bs} , Vt_{bus} and Vt_{refbus}.

The BES control circuit diagram representation is depicted in Figure 2. A two-loop cascaded scheme governs the BDC. By acting on the difference between the reference voltage Vt_{refbus} and the observed bus voltage Vt_{bus}, a PI controller in the outer loop controls the DC link voltage. Its output serves as the BES current reference. The inner loop corrects the discrepancy between the reference and measured BES current by tracking this reference and operating at a higher bandwidth than the outer loop.

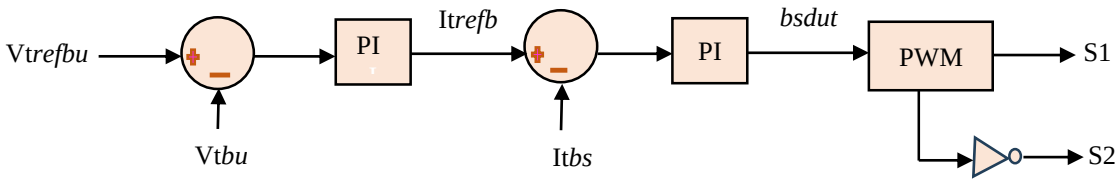


Fig. 2 Control circuit of the energy storage subsystem

By sending the error between reference bus voltage Vt_{refbus} and the bus voltage Vt_{bus} through a PI controller, the outer loop maintains the bus voltage at its fixed value. A second PI controller transforms the current mismatch into the duty cycle bs_{duty}in the faster inner loop using the controller's output as the current reference. The PWM generator generates the complementary gate pulses S1 and S2, and the BDC works in either boost or buck mode according to this duty signal.

The EV charging subsystem interfaces the DC bus with the EV battery through a unidirectional buck type converter. Its components include a stepdown DC-DC converter, an EV charging controller, and an EV battery. The buck type converter manages DC bus power to provide the necessary charging current and voltage. The EV controller continuously records battery voltage Vt_{ev} and charging current It_{ev}. Based on the control error, the PI controller calculates the required duty ratio, which is then applied to the PWM generator to drive the converter switch. As a result, the buck converter maintains the proper charging conditions and provides controlled power to the EV battery. The buck converter for EV charging is regulated using a duty signal $dutyev$ generated by the same cascaded control used in the BES system, which consists of an outer voltage control loop coupled with a high-speed inner current loop as shown in Figure 3.

The EV battery, which serves as the system's electrical load, takes its power primarily from the PV generation unit, with the ESU stepping in to supplement power delivery when PV output is insufficient.

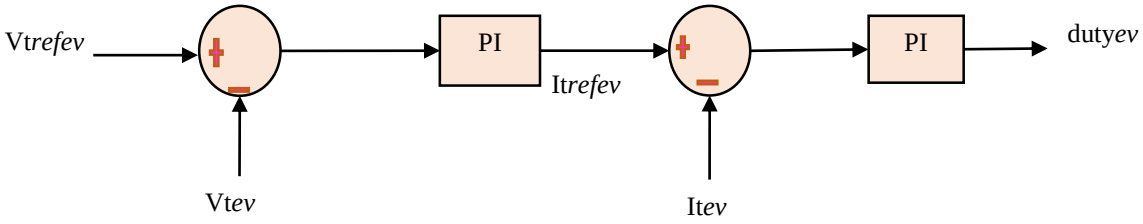


Fig. 3 Buck control circuit of the EV charging subsystem

4. Proposed Attack Modelling Frameworks for EVCS

The standalone EVCS infrastructure is exposed to several cyber threats, including FDI, spoofing, replay, DoS and side channel attacks. The key attack surface in this system is the EV charging subsystem, where both FDI and DoS assaults are used to disrupt normal EVCS operation. This section describes the proposed modelling methodology for these two attack categories.

4.1. Stealthy FDI Attack Modelling Framework

A false data injection assault is a type of cyberattack in which an intruder actively injects modified or invented data into a system with the goal of distorting its operational behaviour or decision-making process. In the EV charging infrastructure, FDI attacks can interfere with sensor measurements, resulting in incorrect charging control, reduced system stability, or unauthorized energy usage [27]. In this work, the FDI attack is carried out by injecting stealthy false data into the EV sensor readings, such as EV voltage Vt_{ev} and current It_{ev} sensors.

Let,

- Vt_{ev}(t) - original EV battery voltage at time t
- It_{ev}(t) - original EV battery current at time t
- $Vt_{ev}\ mod$(t) - modified EV battery voltage at time t after FDI
- $It_{ev}\ mod$(t) - modified EV battery current at time t after FDI
- Nt - total number of timestamps in the dataset.
- α - anomaly injection percentage of timestamps
- $N\ anom$ - number of timestamps chosen to receive anomalies.
- A - set of indices (timestamps) selected for anomaly injection.
- γ_{vt}, γ_{it} - random multipliers used to modify voltage and current, respectively

The number of injected anomaly points is obtained as the product of the total number of timestamps Nt and the anomaly injection fraction α. The value of α is set to 10%, which indicates that injected anomalies are present in 10% of all timestamps in the dataset, as given in Equation (2).

A conscious trade-off between detectability and realism seen in the selection of α = 0.10. Setting α too high (e.g., 30-50%) would misrepresent real world attack behaviour and bias the model toward an unrealistically attack dense operating condition because attacks like FDI and DoS are intrinsically infrequent and discontinuous rather than persistent in practical cyber physical systems. The number of injected anomaly points:

$$N\ anom = \alpha\ .Nt \quad (2)$$

$$A = Randomsample\ (Nt, N\ anom) \quad (3)$$

Let A ⊂ {1, 2, ...Nt} be the set of randomly selected indices where anomalies to be injected are selected. $Randomsample(\{1, \dots, Nt\}, N\ anom)$ takes $N\ anom$ indices without replacement from the set $\{1, \dots, Nt\}$. After this operation $|\ A\ | = N\ anom$. The indices are chosen randomly, simulating sparse and unpredictable false data injection attack events in Equation (3).

The modified voltage $Vt_{ev}\ mod(t)$ is obtained by multiplying the measured EV battery voltage $Vt_{ev}(t)$ by a multiplication factor γ_{vt} for any chosen attack time $t \in A$ in Equation (4). The uniform distribution is the source of the factor $\gamma_{vt} \sim$ U(1.02,1.06). The range 1.02-1.06 indicates a spike attack in which the attacker raises voltage readings by 2%-6%. Stealthy spike anomaly injection at the voltage sensor for every t ∈ {1, 2, ..., Nt}.

If t ∈ A then:

$$Vt_{ev}\ mod(t)\ =\ Vt_{ev}(t)\ .\gamma_{vt} \quad (4)$$

Where γ_{vt} ~U (1.02, 1.06)

Else,

$$Vt_{ev}\ mod(t)\ =\ Vt_{ev}(t) \quad (5)$$

When time t is not in the attack index set A in Equation (5), the voltage stays the same. This ensures that only the chosen timestamps are modified. The current measurement $It_{ev}(t)$ is multiplied by a factor γ_{it} taken from the distribution $\gamma_{it} \sim$ U(0.90,0.96) in Equation (6) for attacked timestamps t. The attacker decreases the EV current by 4% to 10% of the original current value (a drop attack) when the parameter range is 0.90-0.96. The current in Equation (7) remains unaltered if time t is not in the attack index set A.

If t ∈ A, then

$$It_{ev}\ mod\ (\mathrm{t})\ =\ It_{ev}(\mathrm{t})\ .\gamma_{it} \quad (6)$$

Where γ_{it} ~U (0.90, 0.96)

Else,

$$It_{ev}\ mod\ (\mathrm{t})\ =\ It_{ev}\ (\mathrm{t}) \quad (7)$$

Anomaly labelling function output is

$$y(t) = \{1,\ if\ \mathrm{t} \in \mathrm{A}\ \text{or}\ 0, \text{otherwise} \quad (8)$$

Dataset Dt after FDI injection is,

$$Dt = \{(\ Vt_{ev}\ mod(t), It_{ev}\ mod\ (\mathrm{t}), \mathrm{y(t)})|\ t = 1,2, \dots., Nt\} \quad (9)$$

$y(t)$ is the anomaly labelling function output from Equation (8), where 1 indicates that timestamp t was attacked and 0 indicates normal data. Dt represents the dataset after FDI injection, and each timestamp t in Equation (9) captures the modified voltage $Vt_{ev}\ mod(t)$ and the modified current $It_{ev}\ mod$ (t) and the anomaly label $y(t)$.

4.2. DoS Attack Modelling Framework

A denial of service attack aims to degrade or entirely disable the availability of a system, service or network by flooding it with a huge volume of requests or data, leaving it slow, unresponsive or inaccessible to authorized users [28]. The DoS attack model is intended to deliberately interrupt EVCS service availability by reducing the duty cycle of the buck converter to zero, effectively cutting off the power delivery line to the EV battery. Figure 4 displays the resulting duty cycle waveform under three conditions: (a) before the attack, (b) during the DoS event, and (c) after the system is shut down. During normal operation, the duty cycle varies within its normal range, providing for constant power transfer for EV battery charging. When the DoS assault is initiated, the duty cycle is reduced to zero throughout the attack window. This causes the buck converter to stop power conversion completely, reducing the EV charging current to zero. As a result, the charging process is abruptly halted, rendering the EVCS inaccessible to users for the duration of the attack.

The simulation of the DoS attack proceeds as follows,

Step1: Input parameters [duty cycle, time, irradiance, temperature] are fed into the attack block, which is integrated into the buck controller circuit of the EV charging subsystem.
Step 2: Attack triggering conditions are defined by providing thresholds for temperature, irradiance and attack time.
Step 3: Once the threshold conditions are met, the attack is launched by setting the duty cycle to zero $duty_{ev}$ = 0, thereby suspending the charging process.
Step 4: If the trigger conditions are not met, the duty cycle is set to its reference value $duty_{ev}\ = d_{\text{normal}}(t)$ and regular charging occurs.
Step 5: DoS attack makes the EVCS service unavailable to legitimate users.

This modelling approach indicates that setting the buck converter's duty cycle to zero is an effective way to deny EVCS charging service since it completely disables the power transfer path to the EV battery during the attack window. In a practical charger, the EV charging controller generates the duty command of the buck converter and transmits it to the PWM and gate driver stage, while the charging set points are transmitted to the controller through the station's communication interface such as an OCPP connection to a backend server or a CAN or Modbus link from the station controller [4]. If an attacker manages to get access to this interface, they can either block the command messages or bombard the controller with requests. The converter either stops switching or returns to a safe state with no output when the command stream is lost, which is equivalent to a zero-duty cycle. Therefore, the duty command channel between the EV charging controller and the buck converter's PWM generator is considered the attack entry point in this work. The attack block replicates its physical result by overriding the duty command with zero while the trigger circumstances are met.

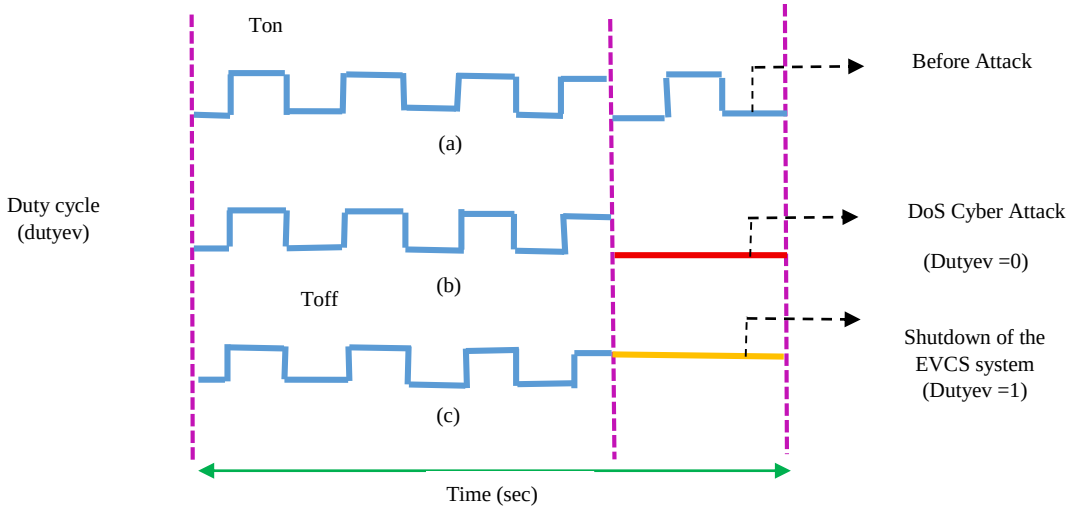


Fig. 4 DoS attack at the duty cycle of the buck type converter in the EV charging module (a) Before attack, (b) During DoS attack, and (c) System shutdown.

5. GRU Based Anomaly Detection Methodology

Anomaly detection is the mechanism of detecting unexpected patterns, irregular events, or outliers in huge datasets that traditional statistical methods may miss. It is often presented as a multiclass classification problem with the goal of labelling data examples as either normal (0), FDI anomalous (1) or DoS anomalous (2). The goal of machine learning-based anomaly detection is to identify observations that deviate from the learnt behaviour by identifying the intrinsic patterns present in a dataset. Anomalies in time series data are observations that significantly deviate from anticipated temporal trends, allowing for the identification of rare or abnormal occurrences such as cyberattacks, equipment faults or sensor malfunctions that remain unnoticed throughout the routine analysis.

This functionality is particularly essential in real-time monitoring applications that require data integrity, such as smart grids, EVCS, and IoT-based systems. Furthermore, machine learning allows for the identification of previously known and unknown anomaly types, boosting the system's overall robustness and detection accuracy. Figure 5 demonstrates the process of GRU-based anomaly detection methodology using a block diagram. Anomaly detection methodology involves steps such as gathering input data, preprocessing data, extracting features, choosing, training, and evaluating machine learning models.

5.1. Gated Recurrent Unit Detection Methodology

GRU enhances the traditional recurrent architecture by introducing two complementary gating mechanisms that govern the preservation and assimilation of temporal information. While the reset gate manages the impact of previous information, the update gate governs the integration of previous information into the present state. Unlike LSTM, GRU eliminates the need for distinct memory cells and instead employs a single hidden state to keep information consistent across the sequence.

The balance between incorporating the newly formed candidate state and keeping information from the previous hidden state is managed by the update gate. z_{t0}. The input vector at time step t is represented by x_{t0}, and the hidden representation propagated from the previous time step is represented by h_{t-1}. The parameters U^{z0} and W^{z0} represent the update gate's recurrent and input weight matrices, respectively whereas b^{z0} represents the bias term as stated in Equation (10).

$$z_{t0} = \sigma(x_{t0}U^{z0} + h_{t-1}W^{z0} + b^{z0}) \quad (10)$$

The degree to which the candidate hidden state is formed by the preceding hidden state is determined by the reset gate r_{t0} It uses the sigmoid activation function to selectively suppress irrelevant historical information.

The parameters U^{r0} and W^{r0} indicate the reset gate's recurrent and input weight matrices, respectively while b^{r0}denotes its associated bias term. The reset gate output is formulated as given in Equation (11).

$$r_{t0} = \sigma(x_{t0}U^{r0} + h_{t-1}W^{r0} + b^{r0}) \quad (11)$$

The current input and the prior hidden state are used to create the candidate hidden state h_t and the reset gate controls the impact of past data. The matrices U^{h0} and W^{h0} represent recurrent and input weight parameters, respectively, while b^{h0} represents the related bias term. Equation (12) presents the hidden state formulation, with $*$ denoting the Hadamard product element.

$$h_t = \tanh(x_{t0}U^{h0} + (r_{t0} * h_{t-1})W^{h0} + b^{h0}) \quad (12)$$

The candidate state h_t and the previous hidden state h_{t-1} are combined, and their respective contributions are regulated by the update gate z_{t0} as defined in Equation (13). This gating procedure allows the GRU to adaptively retain relevant previous information while absorbing new information at the present time step.

$$h_t = (1 - z_{t0}) * h_{t-1} + z_{t0} * h_t \quad (13)$$

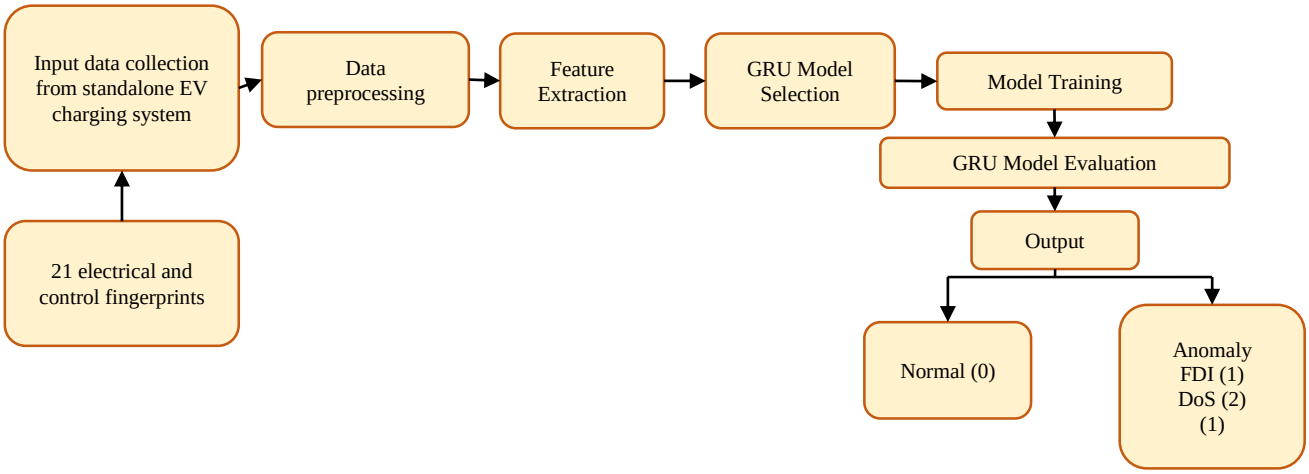


Fig.5 Functional architecture of the GRU based anomaly detection approach

The combined operation of the update and reset gates allows the GRU to selectively save, discard, and incorporate temporal data while preserving a compact network topology. In comparison to LSTM, the absence of a separate cell state results in fewer trainable parameters and reduced processing needs. As a result, GRU may achieve efficient sequence learning while efficiently retaining important information over long temporal intervals and avoiding the vanishing gradient problem seen in conventional RNN. The algorithm for the anomaly detection using GRU is given below in the following steps,

Algorithm 1. Proposed GRU based detection model

1: Instantiate the GRU model using the appropriate design architecture.
2: Set the hidden layers count, activation functions and the layer wise number of neurons.
3: Prepare and organize the dataset for model training and testing.
4: Separate the dataset chronologically into training, validation and evaluation sets.
5: Build 10 sample windows inside each set after fitting the minmax scaler solely on the training months and applying it to all sets.
6: for each training epoch do
7: for every mini batch within the training data do
8: i. Move the input sequence forward through the GRU layers.
9: ii. Determine the loss function.
10: iii. Backpropagate network weights.
11: end for
12: Assess the model for learning rate scheduling and early halting during the validation months.
13: Report the performance indicators for the test months and return the weights of the epoch with the lowest validation loss.
14: end for
15: Utilize the trained GRU model to identify the anomalies on new data
16: Assign the class with the highest softmax probability to each window.
17: Report the detected result outcomes

6. Results and Discussion

The standalone EVCS architecture is developed and simulated using the MATLAB/Simulink software. Machine learning enabled anomaly detection methods are implemented in Python (version 3.7.4) within the Jupyter Notebook interface (version 6.5.4). Solar irradiance and ambient temperature values for the year 2025 specific to the site coordinates of Potheri, India (latitude 12.8204° N, longitude 80.0432° E) are sampled at an hourly resolution to yield 8760 data points from the NASA Prediction of Worldwide Energy Resources (POWER) Data Access Viewer. These meteorological inputs power the PV array model. At each timestamp a set of 21 features is collected from the EVCS, covering electrical and control signal fingerprints, namely [Timestamps, Irradiance, Temperature, Hours, I_{pv}, V_{pv}, P_{pv}, V_{bus}, DC bus current, DC bus power, V_{refbus}, $duty_{pv}$, bs_{duty}, $duty_{ev}$, I_{bes}, V_{bes}, BES SOC, V_{ev}, iev, EV SOC, V_{refev}].

The dataset includes 17,520 hourly samples (15,044 normal, 1,752 FDI and 724 DoS) from two simulation runs using the identical 8,760 hourly weather recordings. The runs differ in terms of sensor noise realizations, FDI and DoS index sets. All model inputs are minmax scaled to [0, 1] with scaling parameters generated solely during the training months. A double layer stacked GRU network is presented for categorizing anomalies into normal, FDI, and denial of service. In contrast to LSTM, GRU maintains a uniform hidden state representation while simplifying the recurrent structure by substituting a single update gate for the input and forget gates, with fewer trainable parameters while maintaining comparable capacity to capture long range temporal dependencies.

The first GRU layer extracts temporal patterns from the 16-dimensional sliding window input using 64 units, while the second GRU layer reduces this representation to 32 units, gradually compressing the sequence encoding into a more discriminative latent form. After each GRU layer, batch normalization is applied to stabilize the distribution of activations and support faster convergence, followed by dropout regularization set at 0.30 after the first layer and 0.15 after the second to mitigate overfitting, with the reduced rate in the deeper layer reflecting its lower risk of over adaptation.

The L2 weight decay ($\lambda = 1\times10^{-4}$) is applied to the kernel and recurrent weight matrices of each GRU layer to reduce model complexity. A dense layer with 32 units and ReLU activation is used after the recurrent block to introduce nonlinear representations before classification. Three Softmax neurons that produce normalized probabilities for the corresponding attack classes make up the output layer. An initial learning rate of 1×10^{-3} is used for the Adam optimization algorithm. The training objective is categorical cross entropy loss, which is usual for multiclass classification. The EVCS is designed under standard test conditions with solar irradiation of 1000 W/m² and an operating temperature of 25°C. The energy storage system includes a Battery Energy Storage (BES) unit with a nominal voltage of 48 V and a capacity of 100 Ah. In addition, the EV load is powered by a Hero Electric lithium ion battery rated at 24 V and with a capacity of 50 Ah.

To represent measurement uncertainty, Gaussian noise was introduced into all sensors in compliance with IEC and IEEE standards. PV side measurements (voltage, current, irradiance, and temperature) are perturbed using tolerances defined in IEC 60051, IEC 61724, and IEC 60751, whereas EV side measurements (battery voltage, battery current) adhere to IEEE instrumentation and control accuracy limits. This ensures that the simulated dataset replicates the unpredictability and drift inherent in real world PV EVCS systems. Each sensor's noise is independently sampled at each time step from the zero mean Gaussian distribution's $\pm3\sigma$ range, which is defined by the tolerance band in Table 3.

6.1. Impact Analysis of Stealthy FDI Attack

The stealthy false data injection attack is emulated by altering 10 percent of the readings obtained from the EV voltage and current sensors. In this model, the EV battery has a nominal voltage rating of 24 V and a fully charged voltage of 27.94 V. The state of charge and internal resistance effects cause the terminal voltage (Vt_{ev}) to rise over the nominal rating during charging. Voltage based FDI produces false readings of 26.29-28.05 V by multiplying the recorded voltage (25.8-26.5 V) by a spike factor of 1.02-1.06. Similarly, a reduction factor of 0.90-0.96 produces falsified current readings of roughly 18-20 A, when the observed EV battery current (It_{ev}) normally ranges from 20 to 21 A.

6.2. Impact Analysis of DoS Attack

The DoS attack is carried out within the buck converter control loop utilizing a specific function block. The block obtains the duty cycle, time, irradiation, and temperature as input variables and generates the duty cycle command for the buck converter. The attack activates when the irradiance is 700-800 W/m², and the temperature is between 25-35°C for 0.4-1s. This disruption makes the EVCS charging service unavailable during the attack. The output characteristic waveforms of both PV and EV before/after DoS attack are shown in Figure 6. The DoS attack is initiated in the buck converter controller circuit at an irradiation of 763.88 W/m^2 and a temperature of 27.28°C are given as inputs to the PV array. The DoS attack is launched from 0.4 s to 1s at each timestamp.

Figure 6(a) depicts the PV voltage before and after the attack. The PV voltage fluctuates briefly during the early startup time due to converter initialization and MPPT settling dynamics. Following the transient interval, the voltage stabilizes at 29 V and remains steady throughout. The steady PV voltage even after the DoS assault shows that the attack

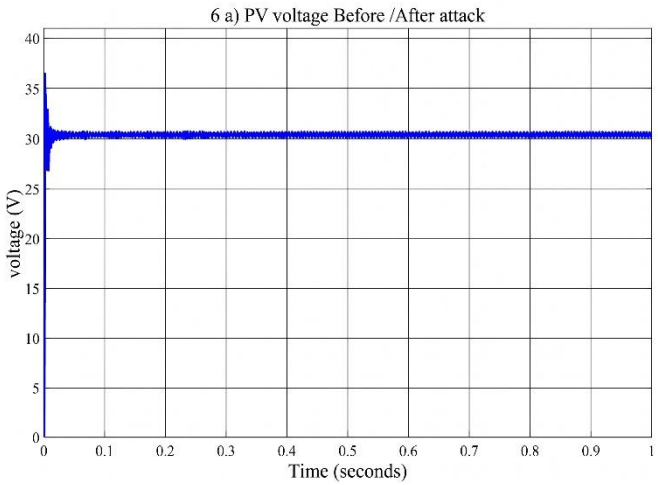
has no effect on the PV generation subsystem. The PV array maintains a steady voltage output since the MPPT controller continues to follow the operating point as normal. Figure 6(b) depicts the PV output current response. Initially, transient variations occur as a result of switching and converter settling. After stabilization, the PV current reaches 23 A and stays constant throughout the simulation. Even after the attack at t = 0.4 s, the PV current does not show any significant changes or instability. This shows that the PV array is operating within normal irradiance and temperature ranges. Figure 6(c) shows the PV output power response before and after the DoS attack. Following the initial transient oscillations, the PV output stabilizes at around 650 W and remains constant over the attack phase. This suggests that the DoS attack affects only the EV charging communication mechanism and not the PV power generation subsystem. During normal operation, the EV battery voltage in Figure 6(d) progressively rises as it charges. However, after the DoS assault begins, the EV voltage remains constant at around 25 V, indicating that the charging process is halted owing to a lack of charging current. Table 2 summarizes the PV array, converter, battery and controller specifications used in the model.

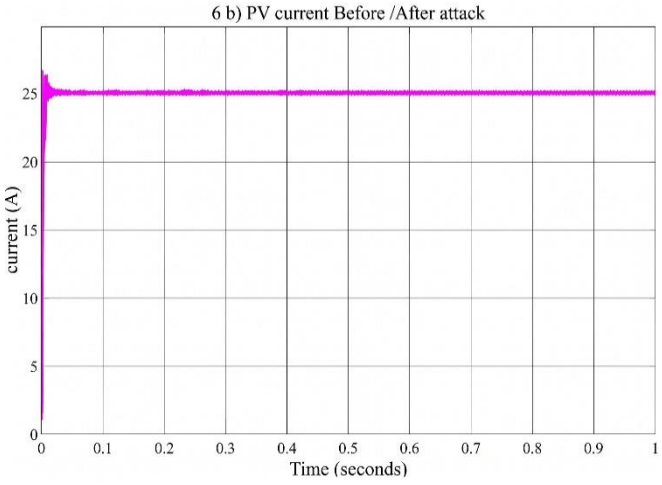
Table 2. System parameters of the EVCS

S. No.	PARAMETERS	VALUES
1.	Parallel PV strings	4
2.	Series module configuration per string	1
3.	Module Name	Suntech Power STP 250-20/wdb
4.	Output Power per panel (W)	250
5.	Cells per module (N cell)	60
6.	Open circuit operating voltageVoc (V)	37.4
7.	Short circuit operating current Isc (A)	8.63
8.	Maximum power voltage Vmp (V)	30.7
9.	Maximum power current Imp (A)	8.15
10.	Inductor /input/output capacitor of PV boost converter	2.2 mH / 55 µF / 40 mF
11.	Switching frequency of the boost converter	20kHz
12.	Inductor / capacitor / switching frequency of BES converter	68 µH / 100 µF / 20 kHz
13.	Reference voltage of DC bus / DC link capacitance	54 V / 100 µF
14.	outer voltage / inner current PI gains of BES controller	K_p = 1, K_i = 10 / K_p = 1, K_i = 1
15.	Inductor / output capacitor / switching frequency of EV buck converter	54 µH / 0.36 mF / 10 kHz
16.	Reference voltage / outer voltage / inner current PI gains of EV controller	24 V / K_p = 1, K_i = 10 / K_p = 1, K_i = 1

Table 3. Gaussian noise added in the sensors of EVCS

Column Name	Noise Range	Standards Reference
V_{pv}	±0.5 - ±1%	IEC 60051 / IEEE 1057
I_{pv}	±1% - ±2%	IEC 60051 / IEEE 1057
Irradiance	±5%	IEC 61724
Temperature	±0.5°C - ±1°C	IEC 60751
V_{ev}	±0.2%- ±0.5%	IEC 60051 / IEEE 1057
I_{ev}	±1%	IEC 60051 / IEEE 1057





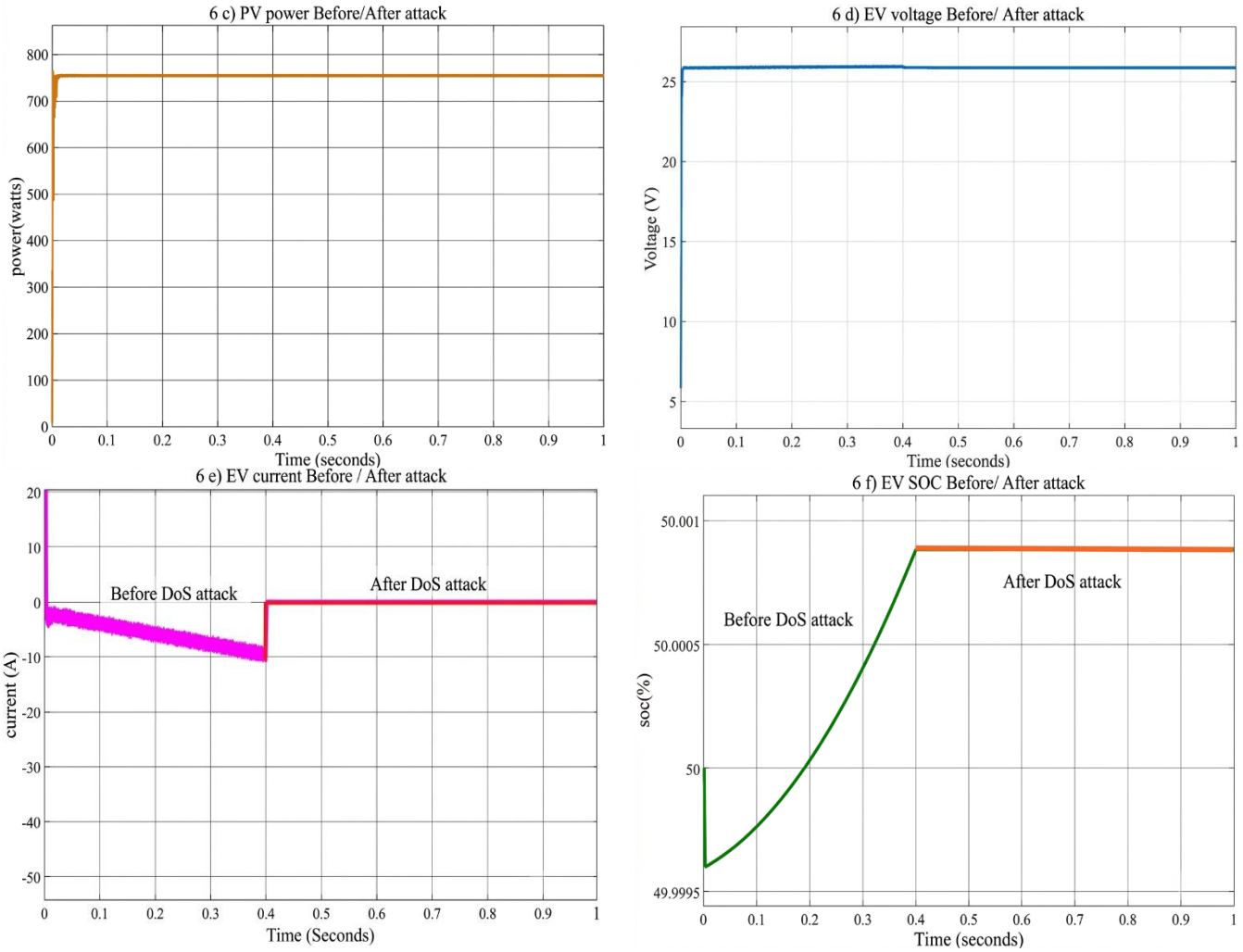


Fig. 6. The output characteristics waveforms of the PV and EV before / after DoS attack of EVCS. (a) PV array voltage, (b) PV array current, (c) PV array power, (d) EV battery side voltage, (e) EV battery side current, and (f) EV battery side SoC.

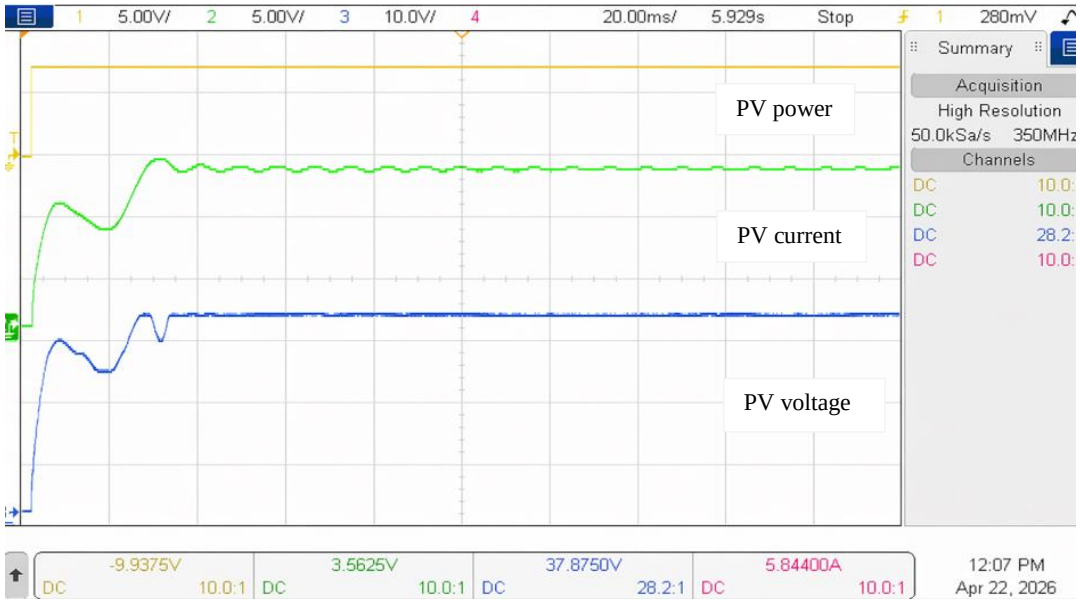


Fig. 7 (a) Output waveforms of voltage, current and power of PV from OPAL - RT before and after DoS attack.

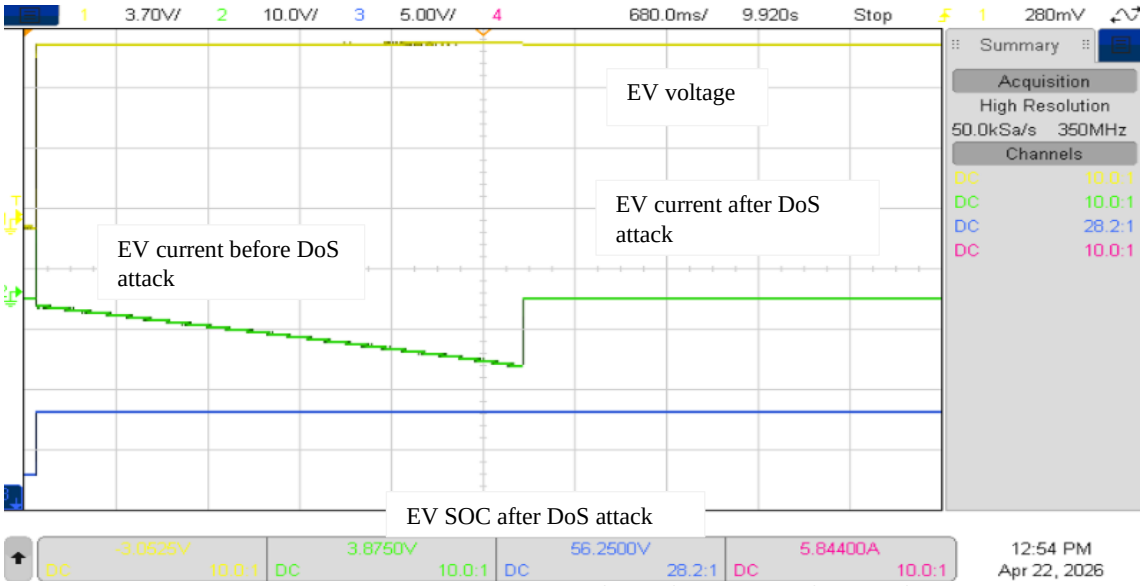


Fig. 7 (b) OPAL - RT output voltage and current waveforms of EV battery before and after DoS attack

The proposed system is implemented and tested using an OPAL-RT real time simulator to emulate the EVCS response under DoS attack in real time. Due to converter switching dynamics and controller setup the OPAL - RT output waveforms of voltage, current and power of PV shown in Figure 7(a) exhibit a transient response with a minor overshoot and oscillatory settling behaviour. However, the voltage and current profiles quickly stabilize, showing the effectiveness of power electronic converters and a correctly tuned closed loop controller developed in the MATLAB environment.

Figure 7(b) presents the OPAL-RT output waveforms of EV battery voltage, current and SOC before and after the DoS attack. The EV battery voltage remains consistent during normal and attack conditions. Before the DoS assault, the EV battery charged regularly, with the charging current gradually increasing. Once the DoS attack begins, the charging current drops to zero, indicating that the charging process has been interrupted.

Consequently, the EV battery SoC increases during normal operation and remains constant after the attack due to a lack of charging current. For real time execution, the MATLAB/Simulink model of the EVCS is interfaced with the OPAL-RT OP4510 real time simulator through RT-LAB. An Intel Xeon processor with five cores is installed in the real time target.

The discrete solver with a fixed time step of 50 µs is used in the simulation. A digital storage oscilloscope attached to the OPAL-RT analog output interfaces is used to track the voltage and current waveforms. The GRU based detection model was then trained and assessed offline using the recorded electrical responses.

6.3. Dataset Preparation, Partitioning and Leakage Control

Every sample in the collection represents a single operating hour. The EVCS model is simulated, and the 21 signals are captured for each hourly pair of irradiance and ambient temperature. The dataset therefore represents hourly operating states rather than the switching level waveforms shown in Figure 6. Three class labels are applied to each sample: Normal (0), FDI (1), or DoS (2).

Samples are labelled with FDI during the predetermined injection window. DoS labels are applied to samples where the attack trigger criteria are met. Of the 21 electrical recorded signals, the timestamp, hour columns and the constant reference signals are excluded to prevent the model from learning the attack schedule from temporal information. The remaining 16 inputs are used as model inputs: [Irradiance, Temperature, I_{pv}, V_{pv}, P_{pv}, V_{bus}, DC bus current, DC bus power, $duty_{pv}, duty_{ev}, I_{bes}$, V_{bes}, BES SOC, V_{ev}, I_{ev}, EV SOC].

Table 4. Window distribution across data partition

Dataset Subset	Window Count	Normal	FDI	DoS
Training Period (January-August)	11,646	10,012	1,148	486
Validation Period (September-October)	2,910	2,428	304	178

Dataset Subset	Window Count	Normal	FDI	DoS
Test Period (November-December)	2,910	2,554	296	60

The dataset is divided chronologically per month instead of using random sampling. The training set covers January to August, the validation set consists of September and October, and the test set consists of November and December. These identical months are chosen from both yearly simulation runs. After fitting the minmax scaler solely on the training set, it is applied to the validation and test sets without any changes. To ensure that no window overlaps samples from two distinct sets, sliding windows of 10 consecutive samples are then individually built inside each set. Every window is labelled with the most recent sample.

Table 4 summarizes the number of windows acquired for each set. Inverse frequency class weights calculated from the training set are used to correct class imbalance. Randomly partitioned overlapping windows and a minmax scaler fitted to the whole dataset were used to further test the GRU model in order to determine the impact of the evaluation technique.

Random partitioning may create data leakage because overlapping windows can exchange raw observations across training and test sets, even though the performance differences for the current dataset were negligible. Additionally, preprocessing incorporates test set information when the scaler is fitted to the entire dataset. The Adam optimizer was used to train all models with a batch size of 32, a maximum of 60 epochs of categorical cross entropy loss and an initial learning rate of 1×10-3. If the validation loss did not improve for ten consecutive epochs, early stopping was used to end training, with the weights from the best performing epoch being restored. When the validation loss remained constant for five consecutive epochs, the learning rate was decreased with a lower bound of 1×10-6. While the other neural network models are assessed over three runs with seeds 0 - 2, the GRU model is assessed over five independent runs with random seeds 0 - 4. For each run, the performance metrics are presented as mean ± standard deviation.

6.4. GRU - AD Performance Analysis

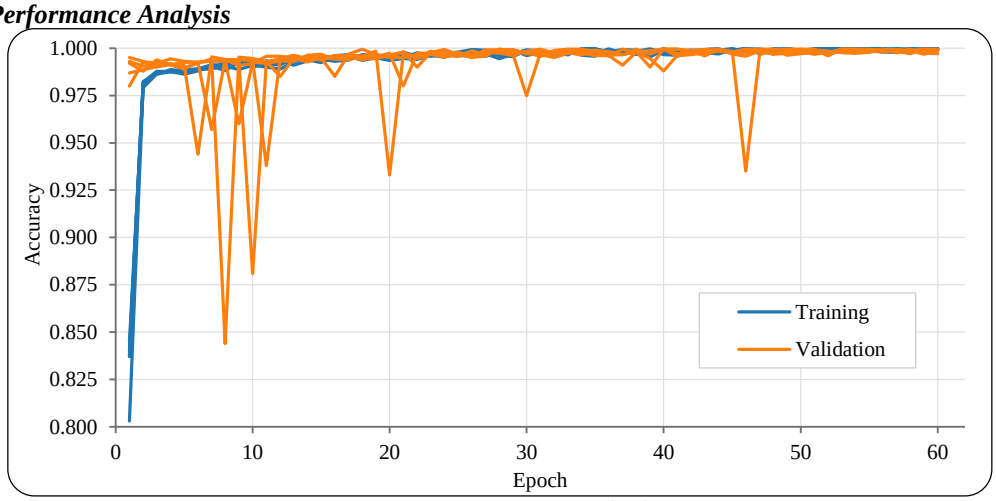


Fig. 8 Training and validation accuracy vs epoch for five runs (seeds 0 to 4)

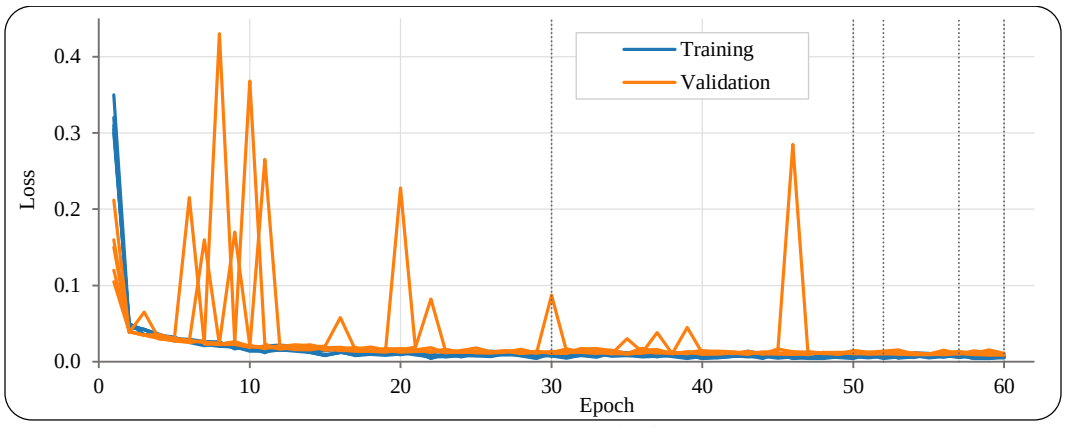


Fig. 9 Training and validation loss vs epoch for five runs (seeds 0 to 4)

The accuracy and loss of the five runs during training and validation are displayed in Figures 8 and 9. During the first few epochs, training accuracy increases above 0.98 and subsequently becomes close to 1.0. The modest number of attacked windows (304 FDI and 178 DoS windows) during the validation months is the cause of these spikes. When a few of these windows are incorrectly identified in one epoch, the validation loss increases dramatically and then decreases in the subsequent epoch. As the learning rate decreases, the spikes disappear.

The model is chosen for each run at the epoch between 30 and 60 that has the lowest validation loss, as shown by the dotted lines in Figure 9. Training achieved the maximum of 60 epochs in four of the five runs. However, in these runs, the validation loss improved by no more than 4.7×10^{-4} over the last ten epochs, which indicates that the epoch limit did not stop training while significant improvement was still occurring. There is no indication of overfitting at the chosen epochs, where the difference between the validation and training losses spans from -0.0009 to 0.0042.

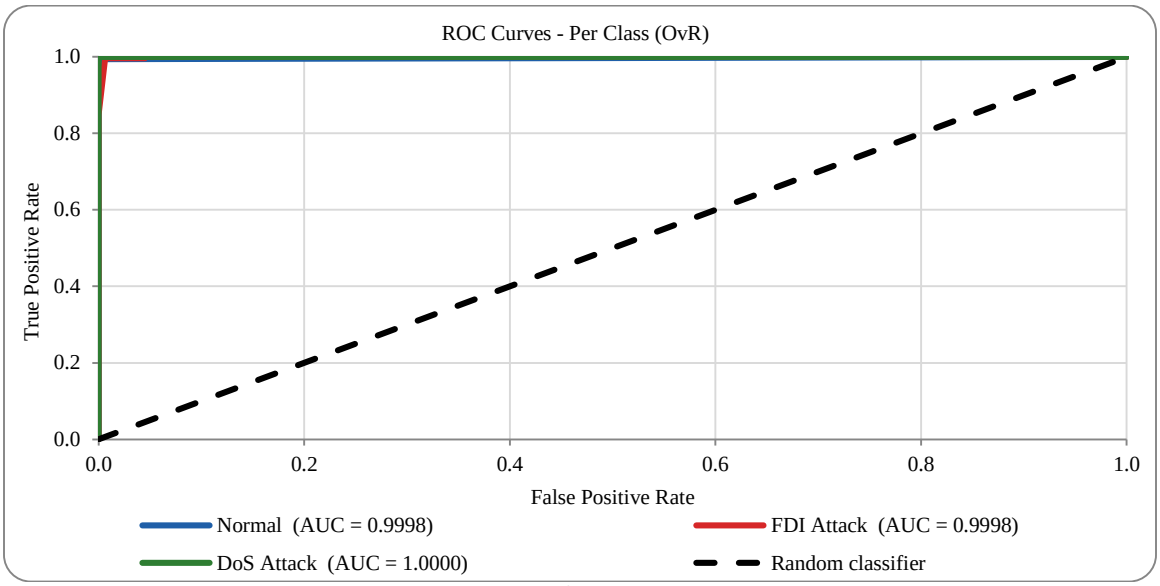


Fig. 10 One vs rest ROC curves of the GRU detector on the test period

		Predicted Label		
		Normal (0)	**FDI Attack (1)**	**DoS Attack (2)**
True Label	**Normal (0)**	2554	0	0
	FDI Attack (1)	2	294	0
	DoS Attack (2)	0	0	60

Fig. 11 Confusion matrix of the GRU detector on the test period (seed 0)

Table 5. Class wise classification metrics of the GRU detector on the test period (mean ± std over five runs)

Class	Precision (%)	Recall (%)	F1-score (%)	FPR (%)	FNR (%)	Support
Normal (0)	99.91 ± 0.02	99.99 ± 0.02	99.95 ± 0.02	0.67 ± 0.14	0.01 ± 0.02	2,554
FDI attack (1)	99.93 ± 0.14	99.19 ± 0.17	99.56 ± 0.14	0.01 ± 0.02	0.81 ± 0.17	296
DoS attack (2)	100.00 ± 0.00	100.00 ± 0.00	100.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	60
Macro average	99.95 ± 0.05	99.73 ± 0.06	99.84 ± 0.05	-	-	2,910
Weighted average	-	-	99.91 ± 0.03	-	-	2,910

Figure 10 illustrates the ROC curves over the five runs. The class wise test month results averaged across five separate runs are shown in Table 5. For every class, the F1-score, precision, and recall are calculated. The weighted average weights each class according to the number of test windows, while the macro average is the unweighted mean of the three class values. For every class, the false positive rate (FPR = FP/ (FP + TN)) and false negative rate (FNR = FN/ (FN + TP)) are calculated. The detector achieves an accuracy of 99.91 ± 0.03%, a macro precision of 99.95 ± 0.05%, a macro recall of 99.73 ± 0.06% and a macro F1-score of 99.84 ± 0.05%. The accuracy varies between 99.86% and 99.93% during the course of the five runs. The FDI class has the most misclassifications, with two of the 296 windows being assigned to the normal class, and all 2,554 normal windows and all 60 DoS windows are correctly classified. In any run, no more than one of the 2,554 regular windows is marked as an attack. The confusion matrix of the best run (seed 0) is shown in Figure 11.

The test months contain only 60 DoS windows from 41 events. With all 60 classified correctly, the exact (Clopper-Pearson) 95% confidence interval for DoS recall is 94.0% to 100%, which confirms reliable DoS detection on this dataset.

6.5. Hyperparameter Sensitivity and Ablation Study

The hyperparameters were assessed one at a time around the chosen configuration with seed 0 and a maximum of 30 epochs per run. The choice is based only on the validation months. The test results in Table 6 are given for information purposes only and were not used in the selection process.

During the validation months, the chosen configuration had the greatest macro F1-score along with a learning rate of 0.0001 and an L2 factor of 0.001. During the test months, the macro F1-score for all settings ranged from 99.62% to 99.87%, indicating that the detector is unaffected by the particular hyperparameter selection. The configuration of (64, 32) units, dropout of (0.3, 0.15), learning rate of 1×10^{-3}, batch size of 32, L2 factor of 1×10^{-4}, and window length of 10 are maintained. A smaller network of (32, 16) units requires only 8,035 parameters and is an appropriate solution for memory-constrained devices.

Table 6. Hyperparameter sensitivity analysis (seed 0)

Parameter	Value	Accuracy (%)	Macro F1 (%)	Params	Train (s)
Units	(32, 16)	99.83	99.68	8,035	104.8
Units	(64, 32)	99.86	99.75	26,691	154.7
Units	(128, 64)	99.86	99.75	96,259	167.3
Window	5	99.79	99.63	26,691	82.6
Window	10	99.86	99.75	26,691	154.7
Window	20	99.90	99.81	26,691	229.5
Dropout	(0.1, 0.05)	99.90	99.81	26,691	152.5
Dropout	(0.3, 0.15)	99.86	99.75	26,691	154.7
Dropout	(0.5, 0.25)	99.90	99.81	26,691	154.4
Learning rate	0.01	99.93	99.87	26,691	153.0
Learning rate	0.001	99.86	99.75	26,691	154.7
Learning rate	0.0001	99.79	99.62	26,691	154.1
Batch size	16	99.86	99.75	26,691	213.2
Batch size	32	99.86	99.75	26,691	154.7
Batch size	64	99.86	99.75	26,691	78.8
L2 factor	0	99.90	99.81	26,691	147.6
L2 factor	0.0001	99.86	99.75	26,691	154.7
L2 factor	0.001	99.86	99.75	26,691	148.9

Table 7. Ablation analysis of input features and architectural components

Variant	Accuracy (%)	Macro F1 (%)	FDI F1 (%)	DoS F1 (%)	Params
Architecture ablation					
Full model	99.89 ± 0.02	99.79 ± 0.03	99.43 ± 0.08	100.00 ± 0.00	26,691
No batch normalization	99.85 ± 0.02	99.73 ± 0.03	99.26 ± 0.08	100.00 ± 0.00	26,307
No dropout	99.90 ± 0.03	99.81 ± 0.05	99.49 ± 0.14	100.00 ± 0.00	26,691
No L2 regularisation	99.84 ± 0.04	99.71 ± 0.08	99.21 ± 0.21	100.00 ± 0.00	26,691
Single GRU layer (64)	99.90 ± 0.03	99.81 ± 0.05	99.49 ± 0.14	100.00 ± 0.00	18,179
No dense layer	99.91 ± 0.02	99.83 ± 0.03	99.55 ± 0.08	100.00 ± 0.00	25,635
No class weights	99.89 ± 0.02	99.79 ± 0.03	99.43 ± 0.08	100.00 ± 0.00	26,691
No temporal window (w = 1)	99.91 ± 0.03	99.83 ± 0.06	99.55 ± 0.16	100.00 ± 0.00	26,691
Feature ablation (number of inputs)					
All features (16)	99.89 ± 0.02	99.79 ± 0.03	99.43 ± 0.08	100.00 ± 0.00	-
Without $duty_{ev}$ (15)	99.90 ± 0.03	99.81 ± 0.05	99.49 ± 0.14	100.00 ± 0.00	-
Without irradiance and temperature (14)	99.86 ± 0.03	99.75 ± 0.05	99.32 ± 0.14	100.00 ± 0.00	-
Without $duty_{ev}$, irradiance, temperature (13)	99.86 ± 0.03	99.75 ± 0.05	99.32 ± 0.14	100.00 ± 0.00	-

Table 7 shows the ablation study's mean and standard deviation throughout three runs (seeds 0 to 2, at most 30 epochs). The entire model achieves a macro F1-score of 99.79 ± 0.03%, whereas variations with one component removed range from 99.71% (no L2 regularization) to 99.83% (no temporal window). All variations are within 0.08 percentage points, corresponding to one or two test windows each run and falling within standard deviations. Batch normalization, dropout, and L2 regularization are kept in place to keep training stable and limit overfitting.

Using a single sample window, the macro F1-score is 99.83 ± 0.06%. At the hourly resolution of this dataset, the current sample already has the majority of the class information; the recurrent window is preserved since attacks evolve over several consecutive samples at the converter time scale, necessitating temporal modelling.

The DoS F1-score remains at 100% in all variations, even when $duty_{ev}$, irradiance, and temperature are deleted, since the detector recognizes the combined signature of a DoS attack, in which I_{ev} goes to zero while the EV SoC stops growing. This demonstrates that DoS detection does not rely on a single input signal.

6.6. Comparative Analysis

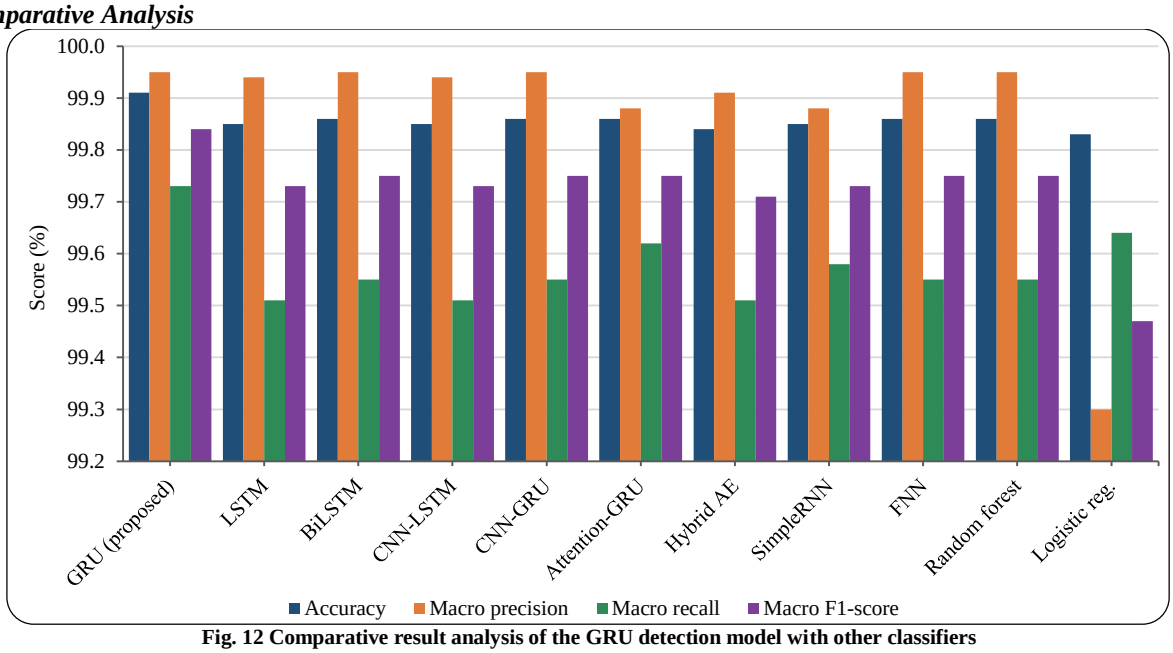


Fig. 12 Comparative result analysis of the GRU detection model with other classifiers

Table 8. Performance comparison of the GRU model with various classifiers

Model	Accuracy (%)	Macro Precision (%)	Macro Recall (%)	Macro F1 score (%)	Params	Train (s)
GRU (proposed)	99.91 ± 0.03	99.95 ± 0.05	99.73 ± 0.06	99.84 ± 0.05	26,691	285.6
LSTM	99.85 ± 0.04	99.94 ± 0.02	99.51 ± 0.14	99.73 ± 0.08	34,307	113.7
BiLSTM	99.86 ± 0.03	99.95 ± 0.01	99.55 ± 0.09	99.75 ± 0.05	84,867	169.7
CNN-LSTM	99.85 ± 0.02	99.94 ± 0.01	99.51 ± 0.05	99.73 ± 0.03	49,731	67.8
CNN-GRU	99.86 ± 0.00	99.95 ± 0.00	99.55 ± 0.00	99.75 ± 0.00	38,659	59.5
Attention-GRU	99.86 ± 0.03	99.88 ± 0.05	99.62 ± 0.10	99.75 ± 0.05	17,555	82.7
Hybrid autoencoder	99.84 ± 0.03	99.91 ± 0.06	99.51 ± 0.06	99.71 ± 0.06	20,467	190.9
SimpleRNN	99.85 ± 0.04	99.88 ± 0.06	99.58 ± 0.11	99.73 ± 0.08	9,443	81.0
FNN	99.86 ± 0.03	99.95 ± 0.01	99.55 ± 0.09	99.75 ± 0.05	24,835	41.4
Random forest	99.86	99.95	99.55	99.75	-	14.2
Logistic regression	99.83	99.30	99.64	99.47	-	0.5

Figure 12 and Table 8 show a comparison of the proposed GRU-based detector to multiple benchmark deep learning models trained on the same dataset, window segmentation approach, train test split, and class-weighting configuration. The proposed GRU attains the best overall performance with an accuracy of 99.91 ± 0.03%, a macro precision of 99.95 ± 0.05%, a macro recall of 99.73 ± 0.06%, and the highest macro F1-score of 99.84 ± 0.05%.

These findings show that the GRU design is good at collecting temporal relationships within converter level measurements and reliably distinguishing between normal operation and cyberattack scenarios. Among the benchmark models, LSTM and CNN-LSTM achieved a macro F1-score of 99.73%, while BiLSTM, CNN-GRU, Attention-GRU, FNN, and Random Forest achieved 99.75%, and the Hybrid Autoencoder 99.71%. Although all competing models performed well, the suggested GRU consistently outperformed the others in terms of overall classification.

Furthermore, the proposed GRU model required only 26,691 trainable parameters, which is significantly fewer than LSTM (34,307), CNN-LSTM (49,731), CNN-GRU (38,659), and BiLSTM (84,867) while maintaining greater detection

accuracy. The GRU's better performance can be due to its gated recurrent structure, which effectively captures temporal properties while reducing the influence of measurement noise inside the analysis window. Overall, the experimental results show that the proposed GRU design effectively captures temporal attack patterns, resulting in better detection performance than competing models while requiring fewer parameters than several recurrent architectures.

6.7. Robustness under Various Operating Conditions

Table 9. Robustness performance of the GRU detector under diverse operating conditions

Scenario	Accuracy (%)	Macro F1 (%)	Detection (%)	False alarm (%)
Test months, noise as in training	99.93	99.87	99.44	0.00
Sensor noise ×2	98.18	96.85	98.03	1.80
Sensor noise ×3	92.96	89.80	96.91	7.60
Irradiance < 300 W/m²	99.95	66.58*	99.55	0.00
Irradiance 300-700 W/m²	99.85	66.38*	98.44	0.00
Irradiance ≥ 700 W/m²	100.00	100.00	100.00	0.00
Temperature < 28 °C	99.96	99.92	99.62	0.00
Temperature ≥ 28 °C	99.80	99.64	98.91	0.00
EV SoC, lower tercile	99.90	99.81	99.16	0.00
EV SoC, middle tercile	100.00	100.00	100.00	0.00
EV SoC, upper tercile	99.90	99.81	99.19	0.00
Unseen: low magnitude FDI (+0.5-2% V, -0.5-2% I)	98.59	97.69	35.00†	0.00
Unseen: voltage-only FDI (+2-6% V)	99.93	99.89	100.00†	0.00
Unseen: current-only FDI (-4-10% I)	97.87	96.41	0.00†	0.00
Unseen: ramp FDI (6-sample drift)	96.74	96.40	68.47†	0.00

Table 9 shows the robustness evaluation of the GRU detector under various operating settings using the model trained with seed 0, with no additional retraining. The detection rate is the proportion of attack windows accurately recognized as FDI or DoS assaults, whereas the false-alarm rate is the percentage of normal windows wrongly classified as attacks.

The proposed detector consistently performs well throughout a wide range of irradiance levels, ambient temperatures, and EV State-of-Charge (SoC) ranges, with accuracy ranging from 99.80% to 100.00%, detection rates ranging from 98.44% to 100.00%, and a false-alarm rate of 0.0%. To assess robustness to measurement uncertainty, the Gaussian noise level applied to the channels indicated in Table 3 was increased to two and three times the nominal value used during dataset construction. Under increased noise levels, the detector-maintained detection rates above 96% despite a decrease in overall accuracy and Macro F1 score.

These findings show that the suggested architecture stays successful at high sensor noise settings despite degrading performance as noise intensity increases. The proposed detector's generalization capability was further tested with previously unseen FDI patterns inserted into normal test samples. The detector detected voltage only FDI attacks at a rate of 100.00% and steady ramp-type attacks at 68.47%. Although detection efficiency varies between attack patterns, the aggregate results show that the GRU model can recognize a wide range of attacker behaviours that are not explicitly represented in the training dataset.

6.8. Computational Cost Analysis

The computational requirements for the proposed detection architecture are provided in Table 10. The model has 26,691 trainable parameters and uses 368 kB of memory. The average training time for five independent runs was 285.6 seconds. During batched execution, the average inference latency was 0.228 ms per window, while single-window processing had an average of 67.4 ms. In addition, all 41 DoS events in the test dataset were recognized on their initial occurrence, resulting in no missed detections. These results reveal that the proposed GRU-based detector has good detection performance with low processing cost, enabling its practical deployment for cyberattack monitoring in standalone EVCS.

Table 10. Computational cost

Item	Value
Trainable parameters	26,691
Model file size	368 kB
Training time	285.6 s (mean of five runs)
Inference, batched	0.228 ms per window
Inference, single window	67.4 ms

7. Conclusion

This paper proposed a gated recurrent unit based detector to identify FDI and DoS attacks in a standalone PV-powered EVCS, which have received comparatively less attention than grid connected and microgrid integrated EVCS. The FDI attacks are introduced to the EV voltage and current sensors, while the DoS attacks on the duty command of the EV buck converter are designed as individual attacks at different times and locations and the resulting effects on the station are assessed using MATLAB/Simulink simulation and on an OPAL-RT real time simulator. Under a leakage free evaluation over five independent runs, the proposed GRU detector achieved an accuracy of 99.91 ± 0.03%, a macro precision of 99.95 ± 0.05%, a macro recall of 99.73 ± 0.06% and a macro F1-score of 99.84 ± 0.05%. Among the benchmark models like LSTM, BiLSTM, CNN-LSTM and CNN-GRU, the proposed detection model achieves the best performance in terms of accuracy and macro F1-score. The proposed GRU model required only 26,691 trainable parameters, which is significantly fewer than LSTM (34,307), CNN-LSTM (49,731), CNN-GRU (38,659), and Bi-LSTM (84,867). Future work will examine the GRU detector's real time deployment on OPAL-RT hardware and evaluate its viability for online cyberattack detection in standalone EV charging systems, as well as its processing needs and detection delay.

Nomenclature

DDoS	Distributed Denial of Service
FDI	False Data Injection
DoS	Denial of Service
PV	Photovoltaic
LSTM	Long Short Term Memory
CNN	Convolutional Neural Network
SVM	Support Vector Machine
AE	Auto Encoder
BES	Battery Energy Storage
PWM	Pulse Width Modulation
AD	Anomaly Detection
ROC	Receiver Operating Characteristics
AUC	Area Under Curve
P_{pv}	PV array power
Vt_{refbus}	DC bus reference voltage
V_{bus}	DC bus voltage
$duty_{pv}$	PV duty cycle
bs_{duty}	Battery energy storage duty cycle
I_{bes}	Battery energy storage current
It_{refbes}	Battery energy storage reference current
Vt_{refev}	EV battery reference voltage
It_{refev}	EV battery reference current
$duty_{ev}$	EV duty cycle
γ_{vt}	Voltage spike
γ_{it}	Current drop
h_t	Hidden state
$tanh$	Activation function

Acknowledgements

G. Sangeetha and D. Suchitra designed the problem under study; G. Sangeetha performed the simulations and obtained the results; G. Sangeetha analyzed the obtained results; G. Sangeetha, D. Suchitra wrote the paper, which was further reviewed by D. Suchitra. All authors have read and approved the final version of the manuscript.

Funding

The authors received no funding for the preparation of this manuscript.

Competing interests

The authors have no competing interests to disclose.

References

[1] A.K.M. Yousuf et al., "An In-Depth Exploration of Electric Vehicle Charging Station Infrastructure: A Comprehensive Review of Challenges, Mitigation Approaches, and Optimization Strategies," *IEEE Access*, vol. 12, pp. 51570-51589, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Deepak Ronanki, and Harish Karneddi, "Electric Vehicle Charging Infrastructure: Review, Cyber Security Considerations, Potential Impacts, Countermeasures, and Future Trends," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 12, no. 1, pp. 242-256, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Samrat Acharya et al., "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, pp. 214434-214453, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen, "OCPP Protocol: Security Threats and Challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452-2459, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] P. Pandiyan et al., "A Comprehensive Review of Advancements in Green IoT for Smart Grids: Paving the Path to Sustainability," *Energy Reports*, vol. 11, pp. 5504-5531, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Zhenhua Yu et al., "A Survey on Cyber-Physical Systems Security," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21670-21686, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Safa Hamdare et al., "Cybersecurity Risk Analysis of Electric Vehicles Charging Stations," *Sensors*, vol. 23, no. 15, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Fatemeh Dehrouyeh et al., "On TinyML and Cybersecurity: Electric Vehicle Charging Infrastructure use Case," *IEEE Access*, vol. 12, pp. 108703-108730, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mansi Girdhar et al., "Hidden Markov Models-based Anomaly Correlations for the Cyber-Physical Security of EV Charging Stations," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3903-3914, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Samrat Acharya et al., "False Data Injection Attacks on Data Markets for Electric Vehicle Charging Stations," *Advances in Applied Energy*, vol. 7, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hamidreza Jahangir, Subhash Lakshminarayana, and H. Vincent Poor, "Charge Manipulation Attacks against Smart Electric Vehicle Charging Stations and Deep Learning-based Detection Mechanisms," *IEEE Transactions on Smart Grid*, vol. 15, no. 5, pp. 5182-5194, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Arif Hussain, Ankit Yadav, and Gelli Ravikumar, "Anomaly Detection using Bi-Directional Long Short-Term Memory Networks for Cyber-Physical Electric Vehicle Charging Stations," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 508-518, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Z.S. Warraich, and Walid Gamal Morsi, "Early Detection of Cyber-Physical Attacks on Fast Charging Stations using Machine Learning Considering Vehicle-to-Grid Operation in Microgrids," *Sustainable Energy, Grids and Networks*, vol. 34, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Tawfiq Aljohani, and Abdulaziz Almutairi, "Modeling Time-Varying Wide-Scale Distributed Denial of Service Attacks on Electric Vehicle Charging Stations," *Ain Shams Engineering Journal*, vol. 15, no. 7, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Yagiz Alp Anli et al., "DDoS Detection in Electric Vehicle Charging Stations: A Deep Learning Perspective Via CICEV2023 Dataset," *Internet of Things*, vol. 28, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Abdurahim Alhashmi et al., "Distributed Denial-of-Service (DDoS) on the Smart Grids based on VGG19 Deep Neural Network and Harris Hawks Optimization Algorithm," *Scientific Reports*, vol. 15, no. 1, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Mhd Ali Alomrani, Mosaddek Hossain Kamal Tushar, and Deepa Kundur, "Detecting State of Charge False Reporting Attacks Via Reinforcement Learning Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10467-10476, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohamed ElKashlan et al., "A Machine Learning-based Intrusion Detection System for IoT Electric Vehicle Charging Stations (EVCSs)," *Electronics*, vol. 12, no. 4, pp. 1-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kirti Gupta et al., "Demonstration of Denial of Charging Attack on Electric Vehicle Charging Infrastructure and its Consequences," *International Journal of Critical Infrastructure Protection*, vol. 46, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Reza Sepehrzad et al., "Enhancing Cyber-Resilience in Electric Vehicle Charging Stations: A Multi-Agent Deep Reinforcement Learning Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 18049-18062, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Yidong Li et al., "Detecting Anomalies in Intelligent Vehicle Charging and Station Power Supply Systems with Multi-Head Attention Models," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 1, pp. 555-564, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Harindra S. Mavikumbure et al., "Cy-Phy ADS: Cyber-Physical Anomaly Detection Framework for EV Charging Systems," *IEEE Transactions on Transportation Electrification*, vol. 10, no. 4, pp. 9904-9917, 2024. [CrossRef] [Publisher Link]

[23] Yang Li et al., "Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862-4872, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mohammad Reza Habibi et al., "Secure MPC/ANN-based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1487-1498, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Suneel Raju Pendem, and Suresh Mikkili, "Modelling, Simulation and Performance Analysis of Solar PV Array Configurations (Series, Series–Parallel and Honey-Comb) to Extract Maximum Power under Partial Shading Conditions," *Energy Reports*, vol. 4, pp. 274-287, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mohammad Haziq Ibrahim et al., "Optimizing Step-Size of Perturb and Observe and Incremental Conductance MPPT Techniques using PSO for Grid-Tied PV System," *IEEE Access*, vol. 11, pp. 13079-13090, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Amirhossein Ahmadi et al., "A New False Data Injection Attack Detection Model for Cyberattack Resilient Energy Forecasting," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 371-381, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Alvin Huseinović et al., "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid," *IEEE Access*, vol. 8, pp. 177447-177470, 2020. [CrossRef] [Google Scholar] [Publisher Link]