Turkish Journal of Science & Technology
20(2), 445-454, 2025

Research Paper
https://doi.org/10.55525/tjst.1656368

Detection of Cyberattacks on Photovoltaic Systems in Smart Grid Infrastructure Using Machine Learning Methods

Usame SAKKAR[1], Ayşe Kübra TATAR[2*]
[1,2] Department of Electrical Engineering, Electrical and Electronics Engineering Faculty, Yıldız Technical University, Istanbul, Türkiye
[2] Clean Energy Technologies Institute, Yıldız Technical University, Istanbul, Türkiye
[1] osama.alsakkar@std.yildiz.edu.tr, [*2] erenayse@yildiz.edu.tr

(Geliş/Received: 12/03/2025; Kabul/Accepted: 01/09/2025)

Abstract: With the increasing concerns over carbon emissions and environmental sustainability, the share of renewable energy sources in power systems has been steadily rising. These systems, which generate variable power depending on meteorological conditions, cause fluctuations in the energy supply-demand balance. Such fluctuations can only be effectively managed through smart grid infrastructure. While smart grids necessitate the integration of communication and information technologies, they also transform power systems into cyber-physical structures, introducing new cybersecurity risks. The integration of distributed generation sources into power systems brings additional cybersecurity threats. Among these threats, false data injection attacks (FDIA) pose significant risks by misleading state estimators (SE), potentially creating severe security vulnerabilities and operational risks. In this study, cyberattacks aiming to manipulate the energy supplied to the grid from photovoltaic (PV) panels and to deceive smartmeter data were analyzed using machine learning-based binary classification methods. The variations in generation levels under low, medium, and high-intensity cyberattack scenarios were modeled using widely adopted algorithms in the literature, including Random Forest Classifier (RFC), XGBoost Classifier (XGBC), and Gradient Boosting Classifier (GBC). The models achieved high accuracy rates, with 92.33% obtained from XGBC in the low-severity attack scenario and 68.59% from GBC in the high-severity attack scenario.

Key words: Cyber-attack, distributed energy resources, machine learning, PV generation, smart grids.

Akıllı Şebeke Altyapısında Fotovoltaik Sistemlere Yönelik Siber Saldırıların Makine Öğrenmesi Yöntemleriyle Tespiti

Öz: Günümüzde karbon emisyonlarının ve çevresel kaygıların artmasıyla birlikte, yenilenebilir enerji kaynaklarının güç sistemlerindeki payı da giderek artmaktadır. Meteorolojik koşullara bağlı olarak değişken güç üretimi gerçekleştiren bu sistemlerin enerji arz-talep dengesinde oluşturduğu dalgalanmalar, ancak akıllı şebeke altyapısıyla etkin bir şekilde yönetilebilmektedir. Akıllı şebekeler, haberleşme ve bilgi teknolojilerinin entegrasyonunu zorunlu kılarken, güç sistemlerini siber-fiziksel yapılara dönüştürerek yeni siber güvenlik risklerini de beraberinde getirmektedir. Dağıtık üretim kaynaklarının güç sistemine entegrasyonu, yeni siber güvenlik tehditlerini de beraberinde getirmektedir. Bu tehditlerin başında gelen sahte veri enjeksiyon saldırıları (False Data Injection Attacks- FDIA), durum tahminleyicilerini (State Estimators- SE) yanıltarak sistemde ciddi güvenlik açıklarına ve operasyonel risklere yol açabilmektedir. Bu çalışmada, fotovoltaik (PV) panellerden şebekeye aktarılan enerjinin manipüle edilmesi ve akıllı sayaç verilerinin yanıltılması yoluyla gerçekleştirilen siber saldırılar, makine öğrenmesi tabanlı ikili sınıflandırma yöntemleriyle analiz edilmiştir. Düşük, orta ve yüksek şiddetli siber saldırı senaryolarına göre değişen üretim miktarları, literatürde yaygın olarak kullanılan Rastegele Orman Algoritması (Random Forest Classifier- RFC), Aşırı Gradyan Artırma Algoritması (eXtreme Gradient Boosting Algorithm- XGBC) ve Gradyan Artırma Algoritması (Gradient Boosting Classifier- GBC) ile modellenmiştir ve yüksek doğruluk oranları elde edilmiştir. Modeller, düşük şiddetteki saldırı senaryosunda XGBC'den 92,33%, yüksek şiddetteki saldırı senaryosunda ise GBC'den 68,59% doğruluk oranı elde ederek yüksek doğruluk oranlarına ulaşmıştır.

Anahtar kelimeler: Siber saldırı, dağıtık üretim kaynakları, makine öğrenmesi, PV üretimi, akıllı şebekeler.

1. Introduction

1.1. Motivation and background

Today's energy systems are undergoing significant transformations due to the rapidly increasing integration of renewable energy sources. In particular, photovoltaic (PV) systems play a crucial role in reducing carbon emissions and promoting environmental sustainability. As of 2022, the global installed capacity of PV systems reached approximately 1070 GW, significantly contributing to reducing dependence on fossil fuels for energy

[*] Corresponding author: erenayse@yildiz.edu.tr . ORCID Number of authors: [1] 0009-0000-6015-1554, [2] 0000-0002-9578-6194

generation [1]. However, the increasing digitalization and integration of PV systems into smart grids have introduced new cybersecurity threats.

Smart grids aim to make energy generation and distribution processes more efficient, reliable, and sustainable by utilizing computer-based automation and remote control technologies [2]. However, as these systems become increasingly dependent on internet-based communication technologies, their vulnerability to cyber-attacks also grows. Smart grids face various cyber threats, such as False Data Injection Attacks (FDIA), Denial of Service (DoS), and Replay Attacks [3].

PV farms, in particular, continuously exchange data with the grid through smart inverters, sensors, and communication hardware. This situation creates new attack surfaces for malicious actors, threatening the stability of energy systems [4]. Cyber-attacks can lead to severe performance degradation by manipulating energy management strategies and disabling control mechanisms [3].

FDIAs are classified as attacks targeting data integrity. Although the destructive potential of such attacks largely depends on the attacker's knowledge of the power grid topology, real-world examples have repeatedly demonstrated their damaging impact [5]. For instance, the 2015 cyber-attack on Ukraine's power grid affected approximately 200,000 customers and caused power outages lasting up to six hours [6]. Similarly, in 2019, an attack targeting the control centers of hydroelectric plants in Venezuela resulted in blackouts across 18 states [7]. In 2010, an attack on Iran's nuclear facilities caused disruptions lasting several hours [8], and the Davis-Besse nuclear power plant in the USA experienced a similar cyber-attack in 2003 [9]. On the other hand, existing algorithms for bad data detection are insufficient for identifying advanced and well-structured FDIA attacks [10]. In this context, data-driven approaches based on machine learning [11-13] have the potential to detect cyber-attacks by directly learning from sensor and meter measurements [14]. However, effectively training these models requires large-scale datasets.

1.2. Literature review

Recent academic studies reveal an increasing use of machine learning methods for detecting cyber-attacks in energy systems. The preference for these methods primarily stems from their ability to directly learn from datasets without requiring explicit mathematical models. For example, in reference [15], a PV system integrated with a battery energy storage system was modeled using MATLAB, and low-magnitude FDIA and DoS attacks were simulated. These attacks were successfully detected using ensemble learning techniques such as Adaptive Boosting (AdaBoost) and Random Forest algorithms with high accuracy rates. In reference [16], historical generation data from a real PV farm in Florida, USA, with a capacity of 1.4 MW, were utilized. Various cyber-attack scenarios created in this study were detected using Support Vector Machines and Recurrent Neural Networks. Reference [17] implemented an unsupervised learning-based recurrent neural network for binary classification to detect cyber-attacks on simulated data from the IEEE 30-bus system.

Considering increasing data sharing and security concerns, reference [18] proposed a federated learning-based approach to detect cyber-attacks targeting power electronics converters in PV farms. In this study, real system data were modeled using OPAL_RT software, and different sensor manipulation scenarios were evaluated. Moradpour and Delkhosh [19] analyzed random ramp attacks on real production data, incorporating weather impacts using symbolic regression methods based on genetic programming and a hybrid probabilistic approach. It is known that manipulating converter input values negatively affects power quality and can lead to harmonic disturbances. In reference [20], a PV system modeled with MATLAB Simulink analyzed the effects of harmonics resulting from the manipulation of converter input values, proposing a detection approach using deep learning-based evolutionary neural networks with transfer learning.

Zhang and Li [21] analyzed attack scenarios where sensor data at the inverter level were manipulated, using Long Short-Term Memory (LSTM) models. Similarly, reference [22] employed data-driven methods based on micro-phasor measurement units to detect cyber-attacks targeting DC/DC and DC/AC converters in a solar energy farm modeled with MATLAB Simulink. In reference [23], deep sequential learning models classified multiple cyber-attacks on converters using data obtained only from a single voltage and current sensor at a common coupling point. This study used multi-layer LSTM networks to analyze the temporal structure of data streams and provided comparative results with various machine learning models. Additionally, reference [24] developed a detection mechanism using convolutional neural networks supported by micro-phasor measurement units and sensor data, testing it across different IEEE bus systems.

Overall, these studies indicate that data-driven machine learning methods effectively detect various cyber-attacks on PV systems. However, considering the dynamic nature of such attacks, it is evident that the adaptive capabilities of current methods need further improvement.

1.3. Contributions and organization of the study

This study investigates the effectiveness of machine learning methods in detecting cyber-attacks targeting PV systems integrated into smart grid infrastructure. Various attack intensities were modeled by creating scenarios where power output data from PV panels and smart meter measurements were manipulated through FDIAs. Commonly used algorithms in the literature, namely Random Forest Classifier (RFC), eXtreme Gradient Boosting Algorithm (XGBC), and Gradient Boosting Classifier (GBC), were comparatively evaluated using datasets obtained under different attack scenarios. This study contributes significantly to the literature by demonstrating the effectiveness of data-driven approaches in securing renewable energy systems.

The remainder of this paper is organized as follows: The Section II provides detailed explanations of the methodology and modeling approach used. In the third section, modeling results and performance analyses are presented. Finally, the Section IV discusses the findings, summarizes the conclusions, and provides suggestions for future research.

2. Methodology

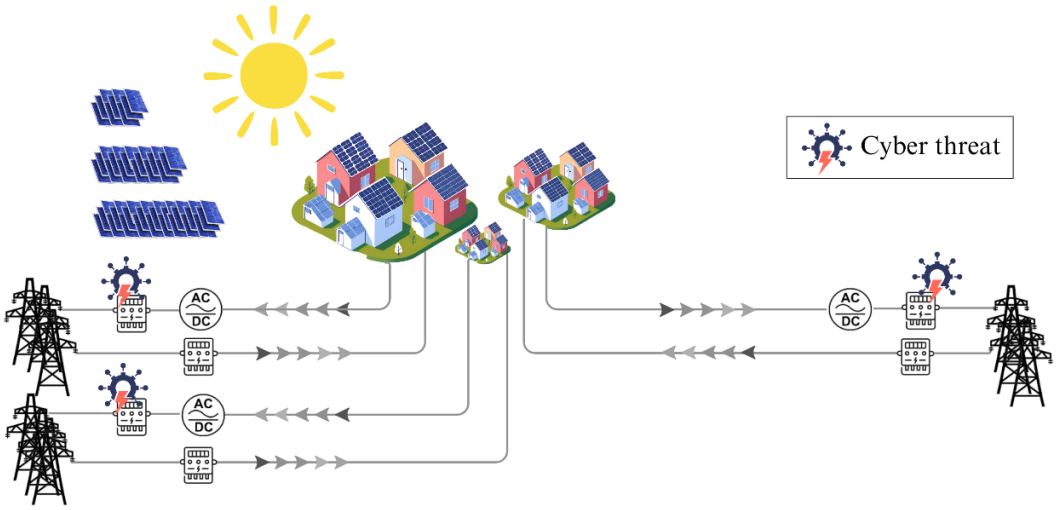

Figure 1. Illustration of a neighborhood-scale smart area comprising residential end-users.

Within the scope of this study, the PV generation profiles of 150 residential customers are analyzed across three distinct rooftop categories, small, medium, and large, corresponding to roof areas randomly selected from the ranges [60, 70, 80, 90], [100, 110, 120], and [130, 140, 150] m², respectively. For each rooftop category, the PV panels are arranged in carefully designed series-parallel configurations that take into account the total available rooftop area per customer. Specifically, rooftops in the small category (60–90 m²) employ 6 parallel groups with 2 panels connected in series, while medium rooftops (90–120 m²) use 6 parallel groups with 3 panels in series. Large rooftops (120–150 m²) are configured with 6 parallel groups and 4 panels in series. This ensures consistency in the electrical characteristics across installations and reflects realistic residential PV layouts.

To synthetically generate the dataset, historical solar irradiance and temperature measurements recorded hourly from May 1, 2024, to May 31, 2024, were obtained from the NASA Prediction of Worldwide Energy Resources database was utilized [25]. These meteorological inputs, combined with the electrical characteristics of 10 different PV panel types used across all residential customers and provided in Table 1, are substituted into Equations (1)–(5) to compute the PV panel's power output [26], which is later used as the target variable in the problem.

The output power of each PV panel type (f) is calculated for each given time point (t) and geographical location (g). Equation (1) is used to calculate the PV cell temperature $T_{g,t,f}^{cell}$ [°C], based on the ambient temperature $T_{t,f}^{A}$[°C], solar irradiance $S_{t,f}^{IR}$ $[kW/m^2]$, and the nominal operating cell temperature $T_{NOCT,f}$ [°C]; the constants 20 and 0.8 represent the standard ambient temperature and the reference solar irradiance used to normalize the cell temperature calculation, respectively.

Table 1. Electrical characteristics of PV panels utilized in the study [27-29].

Model	P_{nom} (W)	NOCT (C°)	V_{mp} (V)	I_{mp} (A)	V_{OC} (V)	I_{SC} (A)	K_V (%°C)	K_I (%°C)	Area (m^2)	Eff. (%)
MAXEON-SPR-3-400	400	45	65.8	6.08	75.6	6.58	-0.236	0.058	1.76	22.6
MAXEON-SPR-3-395	395	45	65.1	6.07	75.4	6.56	-0.236	0.058	1.76	22.3
MAXEON-SPR-3-390	390	45	64.5	6.05	75.3	6.55	-0.236	0.058	1.76	22.1
CanadianSolar-CS3L-325P	325	42	32.0	10.16	39.0	10.74	-0.28	0.05	1.85	17.6
CanadianSolar-CS3L-340P	340	42	32.6	10.43	39.6	10.98	-0.28	0.05	1.85	18.4
CanadianSolar-CS3L-345P	345	42	32.8	10.52	39.8	11.06	-0.28	0.05	1.85	18.7
JA Solar-JAM72S30-530	530	45	41.31	12.83	49.30	13.72	-0.275	0.045	2.58	20.5
JA Solar-JAM72S30-540	540	45	41.64	12.97	49.60	13.86	-0.275	0.045	2.58	20.9
JA Solar-JAM72S30-545	545	45	41.80	13.04	49.75	13.93	-0.275	0.045	2.58	21.1
JA Solar-JAM72S30-550	550	45	41.96	13.11	49.90	14.00	-0.275	0.045	2.58	21.3

The open-circuit voltage $V_{g,t,f}^{OC}$ [V] and the short-circuit current $I_{g,t,f}^{SC}$ $[A]$ are determined by considering both their reference values at standard test conditions and their temperature dependence. Specifically, the open-circuit voltage is calculated using Equation (2) as a function of the reference voltage V_f^{OC} and the voltage temperature coefficient K_f^V [%/°C], adjusted for the difference between the actual cell temperature and the standard 25°C. Similarly, the short-circuit current in Equation (3) depends on the solar irradiance $S_{t,f}^{IR}$, the reference short-circuit current I_f^{SC}, and the current temperature coefficient K_f^I[%/°C], again adjusted relative to 25°C.

After calculating the fill factor FF_f using Equation (4), defined as the ratio of the product of the voltage and current at maximum power point (I_f^{MPP} and V_f^{MPP}) to the product of open-circuit voltage and short-circuit current, the maximum power output of the PV cells $P_{g,t,f}^{PV}$ [W] is determined in Equation (5) by multiplying the fill factor, open-circuit voltage, and short-circuit current.

$$T_{g,t,f}^{cell} = T_{t,f}^{A} + S_{t,f}^{IR} \times \frac{T_{NOCT,f} - 20}{0.8} \tag{1}$$

$$V_{g,t,f}^{OC} = V_f^{OC} \times \left(1 + K_f^V \times \frac{T_{g,t,f}^{cell} - 25}{100}\right) \tag{2}$$

$$I_{g,t,f}^{SC} = S_{t,f}^{IR} \times I_f^{SC} \times \left(1 + K_f^I \times \frac{T_{g,t,f}^{cell} - 25}{100}\right) \tag{3}$$

$$FF_f = \frac{V_f^{MPP} \times I_f^{MPP}}{V_f^{OC} \times I_f^{SC}} \tag{4}$$

$$P_{g,t,f}^{PV} = FF_f \times V_{g,t,f}^{OC} \times I_{g,t,f}^{SC} \tag{5}$$

During the preprocessing phase, all categorical variables were converted into numerical form as an essential initial step. Subsequently, data points with zero solar irradiance were removed to minimize potential bias and ensure that only periods with active solar generation were considered during the training process. In the same context, historical temperature and irradiance data were considered resistant to manipulation and were treated as genuine by machine learning models. However, as depicted in Figure 1, PV generation data for residential users were assumed to be vulnerable to cyber-attacks. Hence, temperature and irradiance served as independent variables, while PV output was the target variable in this binary classification machine learning problem. To ensure transparency, Table 2 presents a detailed description of the dataset features.

To manipulate PV generation data, three cyberattack scenarios with varying intensities and characteristics were developed to simulate realistic actions of malicious customers who manipulate the smart meter data attached to their PV system to falsely overstate their energy injection into the power grid. The attack scenarios are defined as follows:

- Constant Increment Attack (Low Severity)
- Systematic Increment Attack (Medium Severity)

• Random Increment Attack (High Severity)

Table 2. Description of dataset variables.

Variable Name	Role	Type	Description
Customer ID	Metadata	Categorical	Unique identifier assigned to each of the 150 residential customers.
Datetime	Feature	Datetime	The date and hour when the measurement was recorded.
Solar Irradiance	Feature	Numeric (float)	Amount of solar power per unit area (shortwave radiation) reaching the surface, recorded at hourly intervals.
Air Temperature	Feature	Numeric (float)	Ambient air temperature measured 2 meters above ground, recorded at hourly intervals.
Panel ID	Feature	Categorical	Panel ID ranging from 1 to 6, corresponding to six different types of PV panels distributed across 150 residential customers.
Panel Size	Feature	Numeric (float)	Nominal capacity or rated power for each type of the installed PV panels obtained from Table 1.
Number of panels	Feature	Numeric (Int)	Number of rooftop-installed PV panels.
PV Output	Feature	Numeric (float)	Calculated photovoltaic power generated by the installed PV panels for each recorded hour.
Roof Area	Feature	Numeric (float)	Total rooftop area available for PV panel installation.
Attack Flag	Target	Binary (0/1)	Binary label indicating whether the PV output is normal (0) or has been manipulated/attacked (1).

Table 3. Functions utilized to model various cyber-attack scenarios.

Attack Type	Attack Equation	Nature	Severity
Constant Increment Attack	$f_1(PV_{t,f}) = PV_{t,f} + \gamma \cdot P\bar{V}, \quad P\bar{V} \rightarrow Median\ value$		Low
Systematic Increment Attack	$f_2(PV_{t,f}) = PV_{t,f} + \alpha_{t,f} \cdot P\bar{V}, \quad \alpha_{t,f} \sim U(\alpha_{min}, \alpha_{max})$		Medium
Random Increment Attack	$f_3(PV_{t,f}) = PV_{t,f} \cdot (1 + \beta_{t,f}), \quad \beta_{t,f} \sim U(\beta_{min}, \beta_{max})$		High

As presented in Table 3, a total of three scenarios with varying severity and nature are analyzed, with each attack altering half of the data points to maintain balanced classes. Although all attacks are designed to apply a constant magnitude within each scenario, they also exhibit a degree of time dependency in how specific blocks of data, corresponding to particular hours in the dataset's hourly resolution, are selected for manipulation. This is visually described in the Nature column of Table 3. In this visual representation, attacked points are represented in red, and genuine points are uncolored, with each data point corresponding to a specific hour. Additionally, attack magnitudes are randomly chosen from a carefully predefined range and are added to the original data according to the nature of the attack. Randomization in the temporal pattern of attacked blocks or points increases proportionally with attack severity, reflecting the attack's nature. Meanwhile, the magnitude of the added value decreases as severity increases, ensuring that high-severity attacks result in only minimal data disturbances.

In the first scenario, Constant Increment Attack (low severity), a value equal to 0.1 times the median is added to the original data points, targeting only the hours that correspond to even-indexed data points. In the second scenario (medium severity), attacks are applied repeatedly in blocks of equal length, each consisting of two hours of readings, adding a randomly selected value from a uniform distribution ranging between 0.075 and 0.115 times the median to the genuine smart meter readings. Finally, in the high-severity attack scenario, randomly selected blocks of data points, with randomly determined lengths, are manipulated by adding a value drawn uniformly from the range 0.05 and 0.09 times the median.

Python's scikit-learn library is used to develop the machine learning-based attack detection systems. The dataset is split into two sets: 75% for training, and 25% for testing. Out of a total of 66,137 data points, 49,602 are utilized for training, and 16,535 are reserved for testing.

RFC, XGBC, and GBC were selected as the primary machine learning algorithms employed in this study. These algorithms rely on ensemble learning methods, which are known for their high performance and reliable predictive capabilities in classification problems. Ensemble learning combines multiple base estimators to form a single model, resulting in more generalizable and robust predictions.

RFC is a robust ensemble learning method that prevents overfitting by utilizing multiple decision trees trained on various subsets of data and combining the predictions from all trees to make a final classification decision [30]. XGBC and GBC are boosting-based methods that use an iterative approach. Initially, a single decision tree is created, and subsequent trees are iteratively added, each trained to minimize the residuals of predictions made in the previous step. This process continuously enhances model performance, especially for classification problems [31]. To ensure optimal performance, hyperparameter tuning for all models was performed using the GridSearchCV method, with the hyperparameter grid for each classifier thoroughly presented in Table 4.

Table 4. Hyperparameter search grids for all classifiers.

Model Name	Hyperparameter Type	Search Space
RandomForestClassifier	n_estimators	np.random.randint(100, 300, size=5)
	max_depth	[None, 10, 15, 20, 25]
	min_samples_split	np.random.randint(2, 30, size=5)
	min_samples_leaf	np.random.randint(1, 10, size=5)
	max_features	['sqrt', 'log2', 0.3, 0.5, 0.7]
	max_samples	[0.5, 0.75, 1.0]
XGBClassifier	n_estimators	np.array([100, 250, 400])
	max_depth	np.random.randint(3, 15, size=5)
	learning_rate	np.random.uniform(0.001, 0.3, size=5),
	Gamma	[0, 0.5, 1.0, 2.0]
	reg_lambda	[0, 0.1, 1.0, 5.0, 20.0]
	subsample	np.random.uniform(0.5, 1.0, size=5)
	colsample_bytree	np.random.uniform(0.5, 1.0, size=5)
GradientBoostingClassifier	n_estimators	[50, 100, 200]
	learning_rate	[0.01, 0.1, 0.5]
	max_depth	[3, 5, 7]
	subsample	[0.8, 0.9, 1.0]
	min_samples_split	[2, 5, 10]
	min_samples_leaf	[1, 2, 4]

4. Test and Results

In this study, three different cyber-attack scenarios targeting PV systems—low-severity, medium-severity, and high-severity—are examined. The performance of machine learning models is comperatively analyzed based on the nature and severity of each scenario. For a comprehensive evaluation, the Receiver Operating Characteristic (ROC) curve is used, and the optimal classification threshold is determined using Youden's J statistic. Additionally, the metrics of accuracy, precision, recall, and F1 score metrics are employed. All evaluations are conducted using 5-fold cross-validation [32]. The mathematical expressions of the evaluation metrics used are presented in Table 5. To obtain reliable results regarding model performance, a comprehensive testing process is carried out using multiple evaluation criteria. The results obtained from the evaluation metrics for all designed attack scenarios are presented in tables in a structured and sequential manner.

Table 5. Mathematical formulations of applied evaluation metrics.

Evaluation metric	Equation
Accuracy	$\frac{t_p + t_n}{t_p + f_p + t_n + f_n}$
Precision	$\frac{t_p}{t_p + f_p}$
F1 Score	$\frac{2 \times p \times r}{p + r}$
Recall	$\frac{t_p}{t_p + t_n}$

Table 6. Evaluation metrics for the first attack scenario.

Model	Accuracy	Precision	Recall	F1 Score
RFC	0.906133	0.906631	0.906133	0.906104
XGBC	0.923330	0.923482	0.923330	0.923323
GBC	0.882202	0.882544	0.882202	0.882176

The performance evaluation results for the low-severity (Constant Increment) attack scenario are presented in Table 6. In this scenario, the XGBC model achieved the highest performance with an accuracy rate of 92.33%. Moreover, as illustrated in the ROC curve in Figure 2.a), both the XGBC and GBC models demonstrated indentical AUC scores of 0.94, while the RFC model followed with a lower AUC of 0.90.

Table 7. Evaluation metrics for the second attack scenario.

Model	Accuracy	Precision	Recall	F1 Score
RFC	0.789283	0.789461	0.789283	0.789250
XGBC	0.804564	0.804630	0.804564	0.804554
GBC	0.802810	0.802958	0.802810	0.802786

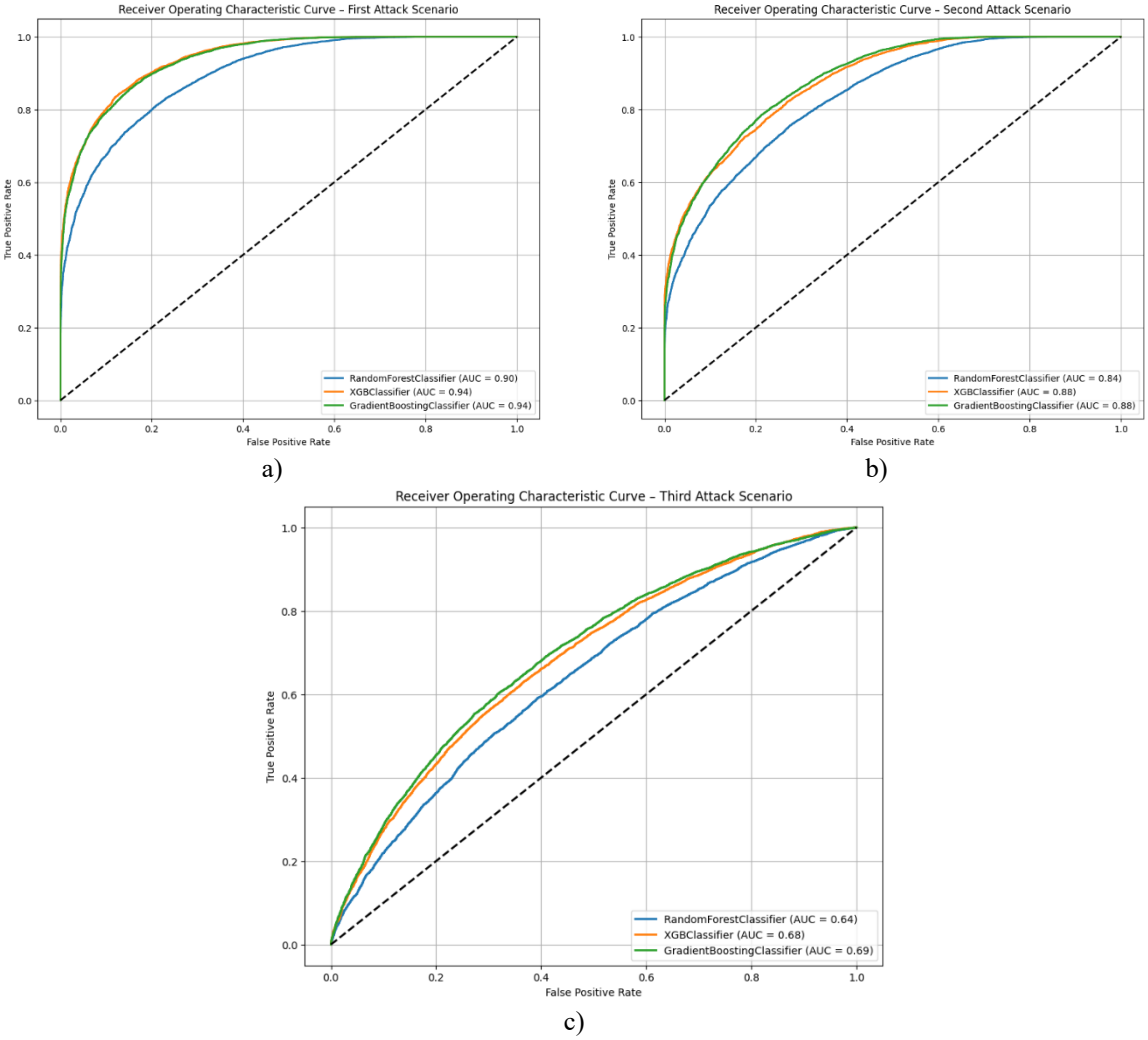

Figure 2. Results obtained from the ROC curve: a) Results derived for the first attack scenario; b) Results derived for the second attack scenario; c) Results derived for the third attack scenario.

Performance evaluation results for the medium-severity (Systematic Increment) attack scenario are provided in Table 7. In this scenario, XGBC and GBC models delivered the best performances, demonstrating superior effectiveness against systematic but partially predictable data manipulations. Upon examining the ROC curve presented in Figure 2.b), it was observed that the XGBC and GBC models achieved the same high AUC values, whereas the performance of the RFC model was notably lower.

Table 8. Evaluation metrics for the third attack scenario.

Model	Accuracy	Precision	Recall	F1 Score
RFC	0.659066	0.659066	0.659066	0.659066
XGBC	0.673602	0.673609	0.673602	0.673598
GBC	0.685859	0.685861	0.685859	0.685859

The results for the high-severity (Random Increment) attack scenario are presented in Table 8. In this randomly and intensively manipulated data scenario, all models exhibited relatively low performance levels; however, GBC model still delivered the best performance. This outcome demonstrates that. The XGBC model ranked second, while the RFC model trailed with the lowest performance. As clearly seen from the ROC curve in Figure 2.c), the performance of all models decreased significantly under this attack scenario.

Boosting algorithm models consistently demonstrated superior performance in all attack scenarios, outperforming tree-based RFC model. This demonstrastes that Boosting algorithms maintain stronger generalization capability when dealing with highly random attacks. In essence, this study highlights the potential of machine learning-based approaches for detecting cyber-attacks of varying intensities and emphasizes the critical importance of selecting appropriate models, particularly in highly complex scenarios.

4. Conclusions, Discussions and Future Work

This study investigated the effectiveness of machine learning-based methods for detecting low, medium, and high-severity cyber-attacks targeting smart meter readings of PV systems integrated into smart grids. RFC, XGBC, and GBC algorithms were selected to analyze attack scenarios categorized as constant increment, systematic increment, and random increment attacks.

Analyses conducted on large-scale datasets generated using real-time meteorological data demonstrated that model performance in attack detection deteriorates as the intensity and randomness of attacks increase. Specifically, a degradation of up to 65.88% for the RFC was observed in the high-severity attack scenario. This highlights both model limitations and the unpredictability of attacks. In practical deployments, modern SCADA and DERMS systems integrate both signal-based and data-driven detection mechanisms that function collaboratively in a complementary manner. Data-driven approaches are particularly vital for detecting attacks that cause minimal signal disturbances but involve significant data manipulation, as seen in Constant Increment and Systematic Increment Attacks. In contrast, when the original data pattern is almost unchanged and no tangible harm is achievable unless attacks are repeated with high frequency—as in high-severity (random increment) attack scenario—the data-driven detection mechanism should be kept active as a backup, while the signal-based detection mechanism operates as the primary system.

The proposed detection mechanism is particularly effective when attacks involve significant data manipulation are launched. It functions alongside other anomaly detection mechanisms already embedded in SCADA environments. Specifically, it can be integrated as a data driven monitoring layer by leveraging existing real-time data streams through standard protocols such as OPC UA or Modbus. The detection algorithm is performed on a systen with 4.60 GHz CPU and 32 GB RAM, showing relatively consistent runtimes across different models, with an average runtime of 223.68 seconds.

For future studies, it is recommended to perform tests on real-time data streams, explore hybrid combinations of different machine learning models to further enhance performance, and evaluate data security for other distributed energy resources and electric vehicle charging stations integrated into smart grid infrastructures, in addition to PV systems.

Acknowlegment

A.K.E-T. contributed to the development of the concept, writing and editing of the manuscript. O.S. performed the simulation studies, interpretation of results and wrote.

References

[1] The International Renewable Energy Agency "IRENA", https://www.irena.org/Publications/2023/Jul/Renewableenergy-statistics-2023. Erişim tarihi: “05.03.2025”.

[2] Fang X, Misra S, Xue G, Yang D. Smart Grid — The New and Improved Power Grid: A Survey. IEEE Commun Surv Tut 2012; 14(4): 944-980.

[3] Guo L, Zhang J, Ye J, Coshatt SJ, Song W. Data-Driven Cyber-Attack Detection for PV Farms via Time-Frequency Domain Features. IEEE T Smart Grid 2022; 13(2): 1582-1597.

[4] Ye J, et al. A Review of Cyber–Physical Security for Photovoltaic Systems. IEEE J Em Sel Top P 2022; 10(4): 4879-4901.

[5] Nguyen T, Wang S, Alhazmi M, Nazemi M, Estebsari A, Dehghanian P. Electric Power Grid Resilience to Cyber Adversaries: State-of-the Art. IEEE Access 2020; 8: 87592-87608.

[6] Eldahshan N, Asif M, Baajaj T, Shaaban MF, Osman AH, Tariq U. A new theft detection approach for cyberattacks in PV generation. 4th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE); 17-19 March 2022; Moscow, Russian Federation. 1-6.

[7] Dehghanian P, Zhang B, Dokic T, Kezunovic M. Predictive Risk Analytics for Weather-Resilient Operation of Electric Power Systems. IEEE T Sustain Energ 2019; 10(1): 3-15.

[8] Wei F, Wan Z, He H. Cyber-attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning. IEEE T Smart Grid 2020; 11(3): 2476-2486.

[9] Haimes YY. On the Definition of Resilience in Systems. Risk Analysis: An International Journal 2009; 29(4): 498-501.

[10] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM T Inform Syst Secur 2011; 14(1): 1-33.

[11] Chaojun G, Jirutitijaroen P, Motani M. Detecting False Data Injection Attacks in AC State Estimation. IEEE T Smart Grid 2015; 6(5): 2476-2483.

[12] Ozay M, Esnaola I, Vural FTY, Kulkarni SR, Poor HV. Machine Learning Methods for Attack Detection in the Smart Grid. IEEE T Neur Net Lear Syst 2016; 27(8): 1773-1786.

[13] Yu, J. J. Q., Hou, Y., & Li, V. O. K. Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks. IEEE T Ind Inform 2018; 14(7): 3271-3280.

[14] Li F, Xie R, Wang Z, Guo L, Ye J, Ma P, Song WZ. Online Distributed IoT Security Monitoring with Multidimensional Streaming Big Data. IEEE Internet Things 2020; 7(5): 4387-4394.

[15] Saiara SA, Ali MH. An ensemble learning based cyber attack detection technique for BESS integrated PV system. SoutheastCon; 15-24 March 2024; Atlanta, GA, USA. 392-397.

[16] Riggs H, Tufail S, Khan M, Parvez I, Sarwat AI. Detection of false data injection of PV production. 2021 IEEE Green Technologies Conference (GreenTech); 7-9 April 2021; Denver, CO, USA. 7-12.

[17] Ayad A, Farag HEZ, Youssef A, El-Saadany EF. Detection of false data injection attacks in smart grids using Recurrent Neural Networks. 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT); 19-22 Feb. 2018; Washington, DC, USA. 1-5.

[18] Zhao L, Li J, Li Q, Li F. A Federated Learning Framework for Detecting False Data Injection Attacks in Solar Farms. IEEE T Power Electr 2022; 37(3): 2496-2501.

[19] Moradpour AM, Alizadeh MH, Delkhosh H. A new method based on symbolic regression to detect the probability of false data injection attacks on PV generation. 2023 13th Smart Grid Conference (SGC); 05-06 Dec. 2023; Tehran, Islamic Republic of Iran. 1-7.

[20] Li Q, Zhang J, Ye J, Song W. Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach. 2022 IEEE Applied Power Electronics Conference and Exposition (APEC); 20-25 March 2022; Houston, TX, USA. 1926-1930.

[21] Zhang J, Li Q, Ye J, Guo L. Cyber-physical security framework for Photovoltaic Farms. 2020 IEEE CyberPELS (CyberPELS); 13-13 Oct. 2020; Miami, FL, USA. 1-7.

[22] Li Q, Li F, Zhang J, Ye J, Song W, Mantooth A. Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data. 2020 IEEE Energy Conversion Congress and Exposition (ECCE); 11-15 Oct. 2020; Detroit, MI, USA. 431-436.

[23] Li F, Li Q, Zhang J, Kou J, Ye J, Song WZ, Mantooth HA. Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network. IEEE T Power Electr 2021; 36(3): 2495-2498.

[24] Zhang J, Guo L, Ye J, Giani A, Elasser A, Song W. Machine Learning-Based Cyber-Attack Detection in Photovoltaic Farms. IEEE Open J Power El 2023; 4: 658-673.

[25] NASA Prediction Of Worldwide Energy Resources (POWER), http://www.ilo.org/global/topics/safety-and-healthatwork/lang--en/index.htm. Accessed: “14.01.2025”.

[26] Masters GM, Renewable and Efficient Electric Power Systems, Wiley Interscience, 2013; 2nd ed. Hoboken, NJ, USA.

[27] Maxeon Solar Technologies, https://sunpower.global/au/sites/default/files/2022-03/sp_max3_112c_blk_410-420_res_dc_ds_en_a4_544456.pdf. Accessed: “16.01.2025”.

[28] Canadian Solar Power, https://www.canadiansolar.com/wp-content/uploads/2019/12/Canadian_Solar-Datasheet-HiKu_CS3L-P_EN.pdf. Accessed: “16.01.2025”.

[29] JA Solar, https://www.jasolar.com/uploadfile/2021/0706/20210706053524693.pdf. Accessed: “16.01.2025”.

[30] Parmar A, Katariya R, Patel V. A review on random forest: An ensemble classifier. International conference on intelligent data communication technologies and internet of things (ICICI); 07–08 Aug. 2018; Coimbatore, India. 758-763.
[31] Scikit learn API, https://scikit-learn.org/stable/api/sklearn.ensemble.html/lang--en/index.htm. Accessed: “09.01.2025”.
[32] Hossin M, Sulaiman M. A Review on Evaluation Metrics for Data Classification Evaluations. Int J Data Mın Model 2015; 5(2): 01-11.