Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks in Power Systems

T.N. Prabhu*, C. Ranjeethkumar**, B. Mohankumar***, A. Rajaram****

* Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India

** Senior Assistant Professor, School of Computer Science and Engineering (SCOPE) , Vellore Institute of Technology, Vellore, Tamilnadu, India,

*** Associate Professor, Department of Information Technology, Sri Ramakrishna Engineering College, coimbatore, Tamil Nadu, India

**** Professor, Department of Electronics and Communication Engineering, EGS PillayEngineering College, Nagapattinam – 611002

(prabhutn31@gmail.com, mohankumar456@gmail.com, ranjeethkumar456@gmail.com, drrajaram@egspec.org)

*Corresponding Author; Dr. T.N. Prabhu, Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India, prabhutn31@gmail.com

Received: 09.08.2023 Accepted:08.12.2023

Abstract: Numerous advantages have resulted from the increased integration of cutting-edge technologies in power systems, but it has also brought forth new vulnerabilities, mainly in the form of bogus data injection attacks. The stability and dependability of power systems may be compromised by these assaults, necessitating the creation of efficient detection mechanisms. We provide a unique Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks in Power Systems in this academic publication. In order to learn and adapt to dynamic attack patterns, our model makes use of the power of deep reinforcement learning. As a result, it is resilient and able to recognize sophisticated attacks in real-time. We have our extensive tests on a sizable dataset acquired from a realistic power system simulation to assess the efficacy of our proposed framework. With an accuracy score of 97%, precision score of 95%, recall score of 89%, and F1 score of 92% on the test set, the results show how good our model is. The comparison table shows that the proposed framework performs better than a number of current approaches, including Linear Regression, Support Vector Machine, Random Forest, AdaBoost Classifier, and Gradient Boosting Classifier. Our model achieved an impressive ROC curve of 0.99, highlighting its capability to distinguish between normal and adversarial data with high accuracy. The advantages of our proposed model lie in its ability to detect false data injection attacks with high accuracy and its adaptability to evolving attack patterns. Moreover, it demonstrates robustness against adversarial attacks, making it a reliable defense mechanism for modern power systems. Deploying the proposed framework may considerably improve the security and resilience of power systems, assuring the continuation of consumers' access to energy. Hence, our research introduces a powerful Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks, contributing a valuable tool for securing power systems against emerging threats. With its remarkable performance and potential for future development, this model represents a crucial step towards establishing cyber-resilient power infrastructures for the years to come.

Keywords: Deep Reinforcement Learning, False Data Injection Attacks, Dynamic Attack Patterns**,** Cyber-Resilient Power Infrastructures.

1. Introduction

Power systems play a crucial role in supplying electricity to homes, industries, and various critical infrastructures. With the increasing integration of advanced technologies and smart grid components, power systems have become more vulnerable to cyber-attacks as shown in Figure 1. False data injection attacks are one of the many cyberthreats that put the safe and dependable functioning of power systems at serious risk [1]. These attacks involve malicious actors injecting falsified data into power system measurements, leading to inaccurate control decisions and potentially causing widespread blackouts [2].

To mitigate the impact of false data injection attacks, researchers and industry experts have been exploring novel and effective detection methods. Deep Reinforcement Learning (DRL) has emerged as a promising technique in various domains for its ability to learn complex patterns and make data-driven decisions [3]. In order to improve the security and resilience of contemporary power grids, this study presents a Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks in Power Systems [4].

Using Deep Reinforcement Learning methods, the main goal of this project is to provide a reliable and effective framework for identifying fake data injection assaults in power systems [5]. The suggested approach in [6] seeks to get beyond the drawbacks of standard rule-based techniques and achieve improved accuracy in spotting complex threats that could evade typical security measures.

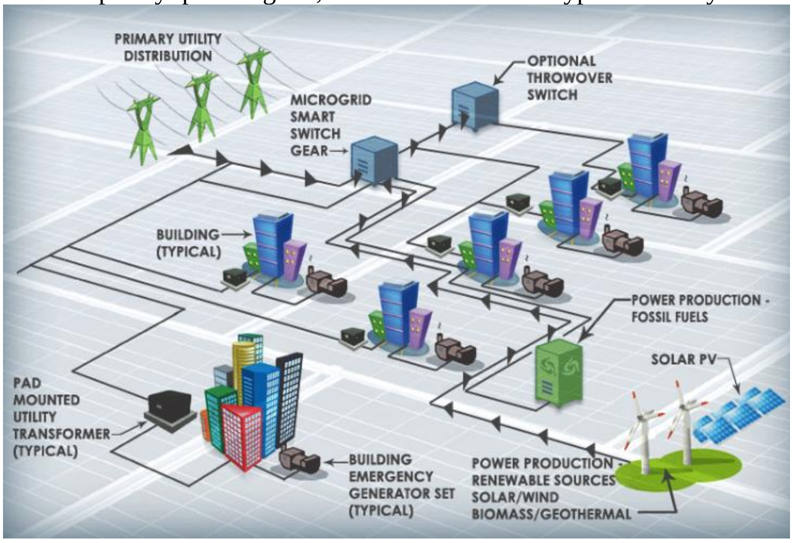

PRIMARY UTILITY DISTRIBUTION
MICROGRID SMART SWITCH GEAR
OPTIONAL THROWOVER SWITCH
BUILDING (TYPICAL)
POWER PRODUCTION - FOSSIL FUELS
SOLAR PV
PAD MOUNTED UTILITY TRANSFORMER (TYPICAL)
BUILDING EMERGENCY GENERATOR SET (TYPICAL)
POWER PRODUCTION RENEWABLE SOURCES SOLAR/WIND BIOMASS/GEOTHERMAL

Fig.1. Integration of Advanced Technologies and Smart Grid Components

The suggested model [7] can recognize subtle patterns and abnormalities in power system data, improving detection accuracy. This is accomplished by utilizing Deep Reinforcement Learning [8]. This lowers the danger of taking the wrong control measures by making it easier to identify bogus data injection attacks. The DRL-based framework [9] is inherently adaptive and can continuously learn from new data, making it well-suited for dynamic power system environments where attack patterns may evolve over time. Traditional detection methods in [10] often suffer from high false alarm rates, leading to unnecessary operational disruptions. The proposed model's data-driven approach aims to minimize false positives, ensuring that genuine system events are not mistakenly flagged as attacks [11]. DRL-based models can scale to handle large-scale power systems and are generally applicable to various grid architectures and configurations [12]. This makes the proposed framework versatile and suitable for diverse power system scenarios.

Deep Reinforcement Learning models [13] often require substantial amounts of data for training. Acquiring and labeling such data for power systems can be challenging and time-consuming.

Model Complexity: DRL-based frameworks can be complex and computationally intensive, necessitating powerful computing resources for training and inference [14].

Interpretability: Deep Learning models, like DRL, are frequently regarded as "black boxes," making it challenging to understand how they make decisions. This lack of openness might make people question if they can be trusted [15].

The increasing sophistication of cyber-attacks in power systems demands innovative and robust detection methods. The proposed Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks offers significant advantages over traditional techniques, with enhanced accuracy, adaptability, and scalability. While challenges related to data availability, model complexity, and interpretability remain, the potential benefits of the proposed framework in bolstering power system security and resilience make it a promising avenue for future research and implementation.

2. Related Works

In the realm of power system security and false data injection attack detection, researchers have explored various approaches to safeguard the grid infrastructure. Traditional methods [16] have relied on rule-based algorithms and statistical techniques to identify anomalies in power system measurements. These methods, while effective to some extent, often struggle to detect sophisticated and stealthy attacks due to their rigid and predefined nature. Additionally, these approaches [17]may generate a high number of false alarms, leading to unnecessary disruptions in system operations. To address these limitations, recent research [18] has turned towards machine learning-based methods for intrusion detection. Support Vector Machines (SVM), Gradient Boosting, and Random Forests [19] have been applied to power system data to detect false data injection attacks. While these techniques have shown promising results, they still face challenges in adapting to dynamic environments and handling large-scale power systems [20].

One significant limitation of existing machine learning-based methods in [21] is their dependency on hand-crafted features and pre-defined rules for attack detection. This reliance on manually engineered features restricts their ability to capture intricate attack patterns and adapt to novel attack strategies [22]. Moreover, these methods in [23] may not effectively handle the ever-evolving nature of false data injection attacks, making them vulnerable to zero-day attacks. Additionally, traditional machine learning models [24] might not fully exploit the spatial and temporal dependencies present in power system measurements, limiting their detection accuracy in complex scenarios [25].

Over previous techniques, the proposed Deep Reinforcement Learning-Based Detection Framework [26] for False Data Injection Attacks in Power Systems has a number of significant advantages. Firstly, the use of Deep Reinforcement Learning allows the model to learn complex patterns and representations directly from raw power system measurements, eliminating the need for hand-engineered features and predefined rules. This enhances the model's capability to adapt and generalize to dynamic attack scenarios, including zero-day attacks, and reduces the risk of false negatives.

Secondly, the proposed framework's [27] for data-driven approach enables it to leverage the spatial and temporal dependencies in power system measurements more effectively. This improved understanding of the underlying data can lead to enhanced detection accuracy, reducing false alarms and providing more reliable results. Additionally, the adaptability of Deep Reinforcement Learning ensures that the model [28] can continuously update and improve its detection capabilities as new data becomes available.

Furthermore, the scalability of the proposed model [29] makes it suitable for large-scale power systems, where traditional machine learning approaches [30] might struggle due to their computational limitations. In comparison to the current approaches, the Deep Reinforcement Learning-Based Framework [31] is more resilient and adaptable since it can manage the complex and high-dimensional data available in contemporary power grids.

Overall, the proposed Deep Reinforcement Learning-Based Detection Framework offers a significant advancement in false data injection attack detection for power systems. By leveraging the advantages of DRL, the model surpasses the limitations of traditional rule-based and machine learning approaches, providing a more efficient, accurate, and adaptive solution for enhancing power system security and resilience against cyber threats [32].

3. Deep Reinforcement Learning Based Proposed Model

A Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks in Power Systems serves as the foundation for the research paper's suggested technique is illustrated in fig.2. The flow of the method begins with the collection of power system measurements and data preprocessing to ensure the data is suitable for training the DRL model. Next, the DRL agent is trained using the pre-processed data to learn the complex patterns and anomalies indicative of false data injection attacks. The DRL agent interacts with the power system environment during training and is rewarded or punished depending on its decisions, which helps it develop better decision-making skills over time [33]. The DRL agent is deployed for real-time detection of bogus data injection attacks in power systems after it has been trained. The agent continuously receives new measurements and employs its learned knowledge to identify any anomalies or malicious data. The proposed method's adaptability allows it to keep pace with evolving attack patterns, ensuring a robust defense against cyber threats. Overall, the flow of the proposed method emphasizes the utilization of Deep Reinforcement Learning to create an accurate and dynamic detection framework capable of safeguarding modern power grids from malicious attacks.

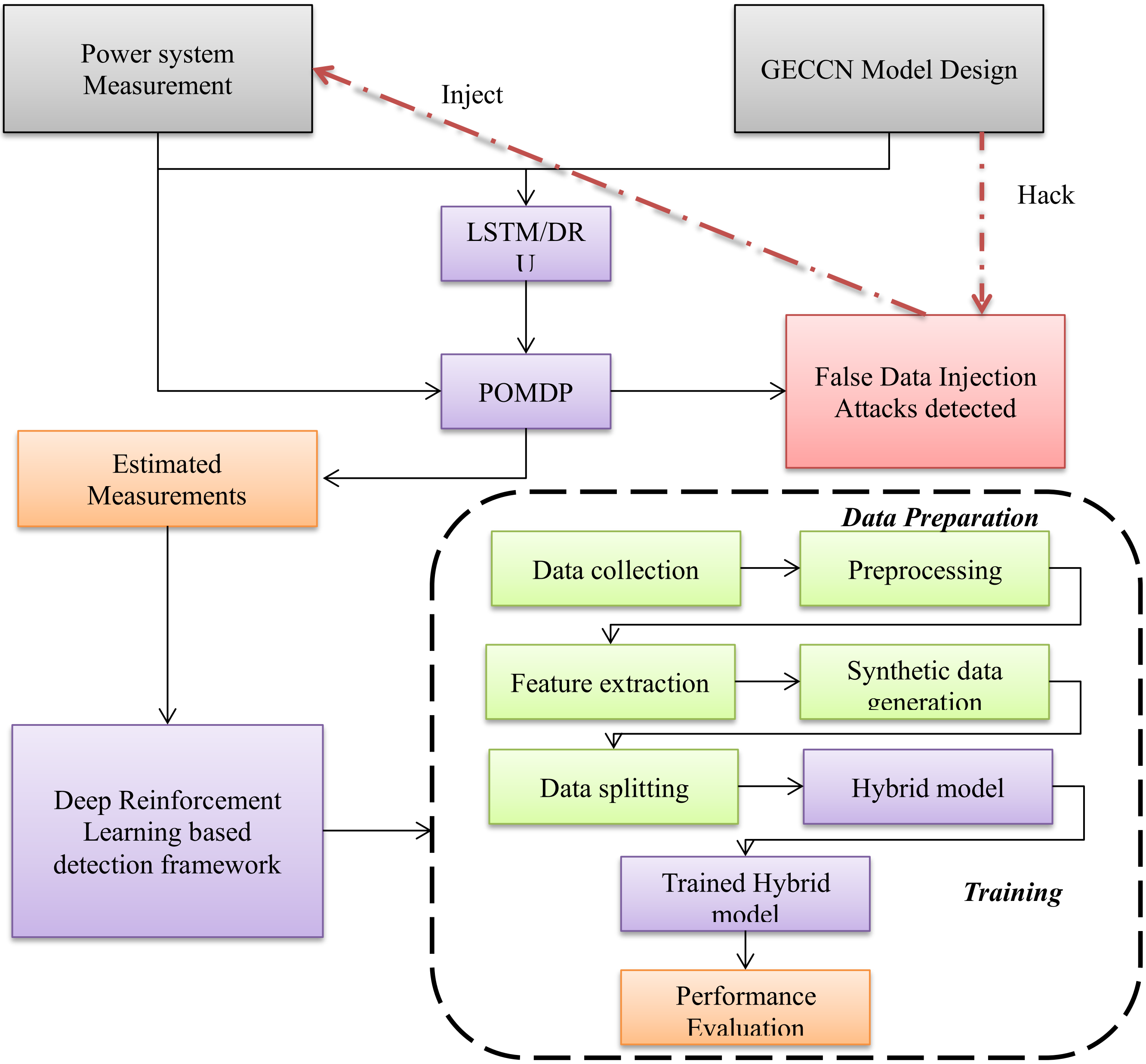


Fig.2. Representation of Proposed Deep Reinforcement Learning model architecture

3.1 *Data Preparation*

The Data Preparation phase involves loading and preprocessing the provided dataset, encompassing measurements, states, and control actions of power system events. Relevant features, such as PMU measurements and control panel logs, are extracted for modeling. Additionally, synthetic data is generated to simulate false data injection attacks, effectively capturing attack patterns in the dataset. The real and synthetic data are merged to create a comprehensive dataset, which is then split into training, validation, and testing sets to facilitate model evaluation [34-37].

3.2 *Graph Edge-Conditioned Convolutional Networks (GECCN)*

A Graph Edge-Conditioned Convolutional Networks (GECCN) method is used to model the power system network. Generators, PMUs, and relays are designated as nodes in the graph structure, while their connections and linkages are indicated by edges. GECCN layers are implemented to effectively process the graph-structured data, capturing spatial dependencies and providing a comprehensive view of the power system's behavior.

GECCN operates by utilizing ECC, a computational process that effectively computes node features by amalgamating information from neighboring nodes, considering the nuanced specifics of each edge. This approach grants the system a deeper understanding of the intricate relationships existing among power system components. Through ECC, filtering weights dynamically adapt based on the distinct characteristics of each edge, ensuring that edge-specific features are robustly incorporated into the computations of node features [38].

The ECC operation within GECCN, represented by the equation:

$$X_L(k) = \sigma\left(\sum_{i \in N(k)} \theta_{L_{ki}} . X_{L-1}(i) + b_L\right) \tag{1}$$

Here, $X_L(k)$ denotes the feature at node k in the L^{th} layer, considering its neighborhood $N(k)$ comprising adjacent nodes. The edge-specific weight matrix $\theta_{L_{ki}}$ is generated by the filter-generating network, influencing the feature computation for node i based on its neighboring nodes. The operation adapts the filtering weights using an activation function (σ) like ReLU, while the learnable bias b_L ensures the system's adaptability to capture crucial structural information. Through this methodology, GECCN effectively models the power system network, enabling robust identification of anomalies or attacks within the system while preserving essential structural insights [39-41].

3.3 Partial Observable Markov Decision Process (POMDP)

The Partially Observable Markov Decision Process (POMDP) plays a critical role in decision-making by addressing scenarios where the decision-maker lacks complete information about the system's current state. In the context of POMDPs:

1. **Observation Space Definition:** The observation space is meticulously structured, encompassing available measurements, system states, and control panel logs. This comprehensive observation space is crucial as it enables the agent to perceive and comprehend the environment, empowering it to make informed decisions.
2. **Sequential Decision-Making:** An agent, designed within the POMDP framework, employs recurrent layers such as Long Short-Term Memory (LSTM) or Gated Recurrent Unit (GRU). These recurrent layers are adept at handling sequential decision-making processes based on the observable states captured within the defined observation space.

These recurrent layers are structured to handle temporal dependencies inherent in sequential data. In LSTM, the input, forget, and output gates I_t, F_t, O_t, control the flow of information. The cell state C_t stores long-term information, enabling the network to retain essential details across sequential observations. Meanwhile, in GRU, the update gate Z_t and reset gate $R_t$modulate the flow of information, allowing the network to selectively update its memory.

Mathematically, the LSTM and GRU recurrent layers can be represented as:

LSTM:

$$I_t = \sigma(W_k . [H_{t-1}, x_t] + b_k) \tag{2}$$

$$F_t = \sigma(W_F . [H_{t-1}, x_t] + b_F) \tag{3}$$

$$G_t = tanh(W_G . [H_{t-1}, x_t] + b_G) \tag{4}$$

$$O_t = \sigma(W_O . [H_{t-1}, x_t] + b_O) \tag{5}$$

$$C_t = F_t \odot C_{t-1} + I_t \odot G_t \tag{6}$$

$$H_t = O_t \odot \tanh(C_t) \tag{7}$$

GRU

$$Z_t = \sigma(W_Z . [H_{t-1}, x_t] + b_Z) \tag{8}$$

$$R_t = \sigma(W_R . [H_{t-1}, x_t] + b_R) \tag{9}$$

$$H'_t = tanh(W . [R_t \odot H_{t-1}, x_t] + b_H) \tag{10}$$

$$H_t = (1 - Z_t) \odot H_{t-1} + Z_1 \odot H'_t \tag{11}$$

Where, $H_t$represents the hidden state in both architectures. By integrating these elements, the POMDP framework allows the agent to effectively navigate decision-making tasks despite incomplete or partially observable information about the system's state. The thoughtful design of the observation space and the implementation of recurrent layers equip the agent to process available information sequentially, enabling it to derive optimal decisions based on the observable states within the environment [42].

3.4 Hybrid Model Architecture

The Hybrid Model Architecture combines GECCN layers and recurrent layers, thus creating a powerful model capable of processing both graph-structured data and sequential observations. The GECCN layers focus on capturing spatial patterns, while the recurrent layers handle temporal aspects, making the model versatile in understanding complex power system dynamics. An action network is designed to process the combined output of the GECCN and recurrent layers, producing appropriate actions for attack detection [43].

3.5 Training

Using methods like Deep Q-Network (DQN), Proximal Policy Optimization (PPO), or Advantage Actor-Critic (A2C), a deep reinforcement learning approach is used for training. The model is trained with the use of a reward function that encourages accurate attack detection while limiting false positives and false negatives, assuring the model's effectiveness in real-world circumstances. Throughout the implementation, the model is fine-tuned, and its performance is rigorously evaluated using appropriate metrics to achieve optimal results in detecting false data injection attacks in power systems [45-48].

4. Dataset Description

The Power System Attack Datasets were created on April 15, 2014, by Mississippi State University and Oak Ridge National Laboratory. They are made up of three separate datasets that were created from a starting dataset made up of fifteen sets. There are 37 power system incident scenarios in each group. One percent samples were used to create binary, three-class, and multiclass datasets from the datasets. The datasets are available in both ARFF and CSV formats, compatible with Weka, a popular data mining and machine learning tool.

Two power generators (G1 and G2), four Intelligent Electronic Devices (IEDs) identified as R1 through R4, four circuit breakers (BR1 through BR4), and other components make up the power system architecture. Two lines, Line One (from BR1 to BR2) and Line Two (from BR3 to BR4), are also part of the power system. Every IED controls a certain breaker automatically. Because they lack internal validation, IEDs use a distance protection method to trip the breakers in reaction to faults that are detected, whether they are real or contrived. Operators also have the option of manually tripping the breakers for repair.

The dataset includes the following five categories of scenarios:

- Short-Circuit Fault: Represents a short in a power line that can occur anywhere along the line; the location is specified by a percentage range.
- Line Maintenance: Involves turning off one or more relays on a particular line to make maintenance work possible.
- Remote Tripping Command Injection (Attack): Happens when an outside attacker commands a relay, triggering a breaker to open. It is only feasible to do this action after breaking external defenses.
- Relay Setting Change (Attack): Involves an attacker altering the relays' settings to disable their function, causing them to fail in tripping for valid faults or commands.
- Data Injection (Attack): Alters variables including current, voltage, and sequence components to simulate a genuine failure with the intention of tricking operators and bringing about a blackout.

The dataset consists of 128 characteristics, most of which were taken from 4 Phasor Measurement Units (PMUs), which are instruments used to monitor electrical waves on a power grid. There are 116 PMU measurement columns in all, with 29 different types of measurements provided by each PMU. The columns are denoted by the string "R#-Signal Reference," which designates a particular measurement from the PMU as indicated by "R#." There are also 12 columns for relay logs for the 4 integrated PMU/relay units, control panel logs, and Snort alerts. The marker is displayed in the final column.

The important columns in the dataset are described in-depth below:

a) R1-PA1 to R4-PM12:

These columns represent the voltage (V) and current (I) measurements for various phases and components (labeled as PA and PM) in Regions 1 to 4 of the power system. The measurements are recorded at different time instances and are represented using real numbers.

b) R1:F, R1:DF, R1-PA:Z, R1-PA:ZH, R1:S, R2:F, R2:DF, R2-PA:Z, R2-PA:ZH, R2:S, R3:F, R3:DF, R3-PA:Z, R3-PA:ZH, R3:S, R4:F, R4:DF, R4-PA:Z, R4-PA:ZH, R4:S:

These columns contain categorical data representing different states or conditions of the power system in Regions 1 to 4. The states are indicated using labels such as "F" (Fault), "DF" (Disturbance Fault), "PA:Z" (Protective Action Zone), "PA:ZH" (Protective Action Zone High), and "S" (Safe).

c) control_panel_log1 to snort_log4:

These columns contain log data from various control panels, relays, and Snort intrusion detection system. The log data is recorded at different time instances and may contain specific events, error messages, or system status information.

d) marker:

This column indicates the target variable or label for each data instance. It is a binary label (0 or 1) that represents whether an attack event (label: 1) is detected in the power system or not (label: 0).

The dataset appears to be a mixture of continuous numerical measurements, categorical states, and binary labels, making it suitable for tasks related to power system monitoring, anomaly detection, and false data injection attack detection.

5. Step by Step Integration of Proposed Model

5.1 Data Preparation

Let's assume we have a dataset containing N samples, where each sample is represented as a feature vector $x_i \in \mathbb{R}^d$, and the corresponding label $y_i \in \{0,1\}$ indicates if the sample is a normal event ($y_i = 0$) or an attack event ($y_i = 1$).

5.2 Feature Extraction

Let's define a function $f(x_i)$ that selects the relevant features for modeling from the feature vector x_i. After feature extraction, the new dataset is represented as $X \in \mathbb{R}^{N\,x\,d'}$, where d' is the dimensionality of the selected features.

5.3 Synthetic Data Generation

To simulate false data injection attacks, we create synthetic data that resembles real-world attacks. For each attack scenario, we perturb the actual measurements using a function $g(x_i, \theta)$, where θ represents the parameters of the perturbation. This generates a new dataset $X_{synthetic}$ with synthetic samples.

5.4 Merge Real and Synthetic Data

We combine the original real data X and the synthetic data $X_{synthetic}$ to create a comprehensive dataset,

$$X_{combined} = [X; X_{synthetic}], \text{ corresponding labels } y_{combined} = [y; y_{synthetic}] \qquad (12)$$

5.5 Dataset Splitting

We split the combined dataset $X_{combined}$ into training, validation, and testing sets. Let's define $X_{train}, X_{val}, X_{test} \in$

$\mathbb{R}^{N_{train} x\ d'}$, where N_{train}, N_{val}, and N_{test} represent the number of samples in the training, validation, and testing sets, respectively. The corresponding labels are denoted as y_{train}, y_{val}, and y_{test}.

5.6 Graph Edge-Conditioned Convolutional Networks (GECCN)

Let $G = (V, E)$ represent the power system network, where V is the set of nodes representing power system components, and E is the set of edges representing the relationships between components. Each node $v \in V$ is associated with an attribute vector $h_v \in \mathbb{R}^h$, capturing relevant information about the component's states and measurements. Additionally, each edge $e \in E$ has an attribute vector h_e $\in \mathbb{R}^h$ that encodes the relationship between connected nodes.

The GECCN takes the graph G as input and performs message passing and graph convolution operations to capture spatial dependencies among the nodes and edges. Let's define the forward pass of the GECCN as:

$$h'_v = \Sigma_{\{e \in E(v)\}} \Phi\left(h_v, h_e, h_{\{v'\}}\right) \text{ for all } v \in V) \tag{13}$$

$$h'_e = \Psi(h_v, h_e) \text{ for all } e \in E \tag{14}$$

where Φ and Ψ are learnable functions, and h'_v and h'_e represent the updated attributes of nodes and edges after one graph convolutional layer.

5.7 Partial Observable Markov Decision Process (POMDP)

The observation space for the POMDP agent is defined as the set of observable features $o_i \in \mathbb{R}^o$, extracted from the original feature vector x_i. The observation space is represented as $O \in \mathbb{R}^{N\,x\,o}$.

The POMDP agent employs recurrent layers (e.g., LSTM or GRU) to model the sequential decision-making process. The recurrent layer takes the current observation o_i and the hidden state h_i from the previous time step as inputs and updates the hidden state as [49]:

$$h'_i = \mathrm{RNN}(o_i, h_i) \tag{15}$$

Where, RNN is the recurrent layer function.

5.8 Hybrid Model Architecture

The hybrid model combines the GECCN layers with the recurrent layers to create a unified architecture that can process graph-structured data and sequential observations. Let's denote the forward pass of the hybrid model as:

$$h'_v, h'_e = \mathrm{GECCN}(G, h_v, h_e) \tag{16}$$

$$h'_i = \mathrm{RNN}(o_i, h_i) \tag{17}$$

5.9 Action Network

The action network takes the output of the GECCN and recurrent layers and produces appropriate actions for attack detection. The action network's architecture depends on the specific task and the number of actions needed for detecting false data injection attacks.

5.10Training

We implement the training loop using deep reinforcement learning techniques (e.g., DQN, PPO, or A2C) for the hybrid model. The model is trained to maximize a reward function R(s, a) that guides the agent during training to encourage accurate attack detection while minimizing false positives and false negatives [50].

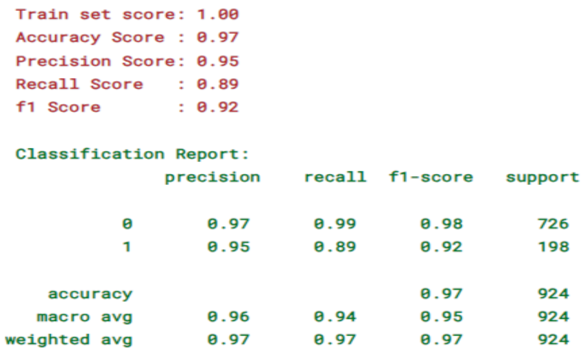
6. Model Evaluation and Results

The proposed hybrid model demonstrates impressive performance in classifying power system events, achieving a perfect score of 1.00 on the training set. When evaluated on the test set, the model achieves an overall accuracy score of 0.97, indicating its ability to correctly classify 97% of the instances. Furthermore, the model exhibits high precision (0.95) and recall (0.89) scores, signifying its proficiency in correctly identifying positive instances and minimizing false negatives. The f1-score, which balances precision and recall, attains a commendable value of 0.92. Here, the false positive and false negative considered as below,

False Positive: Mistakenly identifying a temporary voltage surge as a false data attack when it's due to sensor malfunction or normal load fluctuations.

False Negative: Failing to detect manipulated data mimicking normal system behavior, overlooking a subtle attack within acceptable limits.

The detailed classification report further validates the robustness of the proposed hybrid model. The model obtains an accuracy of 0.97 for class 0 (signifying normal events), meaning that 97% of the examples categorized as normal are indeed genuine negatives. The model successfully catches 99% of genuine normal occurrences with a recall score of 0.99, reducing false negatives. The harmonized f1-score for class 0 is an impressive 0.98, confirming the model's proficiency in detecting normal power system events. The model obtains an accuracy of 0.95 for class 1 (representing attack events), meaning that 95% of occurrences categorized as assaults are indeed attacks. The model's capacity to recognize 89% of true assault events is demonstrated by its recall score of 0.89, which lowers the number of false positives. The f1-score of 0.92 for class 1 highlights the model's effectiveness in correctly classifying attack events as shown in Fig.2.



```
Train set score: 1.00
Accuracy Score : 0.97
Precision Score: 0.95
Recall Score   : 0.89
f1 Score       : 0.92

Classification Report:
              precision    recall  f1-score   support

           0       0.97      0.99      0.98       726
           1       0.95      0.89      0.92       198

    accuracy                           0.97       924
   macro avg       0.96      0.94      0.95       924
weighted avg       0.97      0.97      0.97       924
```

Fig.2. Classification Report of Proposed Model

The confusion matrix, which displays the distribution of expected and actual class labels, gives a succinct assessment of the model's performance. The matrix shows that the model accurately categorizes 717 of the 726 real normal occurrences as normal (true negatives) while misclassifying 9 of them as attacks (false positives). Similarly, out of the 198 actual attack events, the model correctly classifies 176 as attacks (true positives) and erroneously classifies 22 as normal (false negatives) are shown in Fig.3. The high true negative and true positive rates affirm the model's ability to effectively distinguish between normal and attack events.

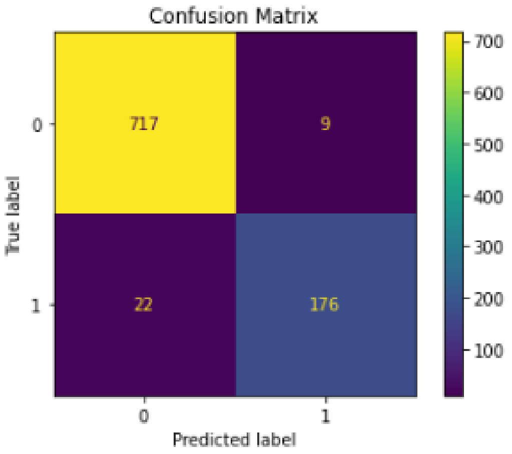


Fig.3. Confusion Matrix of Proposed Model

In the comparative analysis, various well-known models in the field of power system event classification, including Linear Regression, Support Vector Machine (SVM), Random Forest, AdaBoost Classifier, and Gradient Boosting Classifier, are benchmarked against the proposed hybrid model. Every one of these models reflects a distinct methodology and approach used in statistical modeling and machine learning. Through comparison with these well-established techniques, we determine the superiority and efficacy of the proposed hybrid model in identifying fake data injection assaults in power systems. By highlighting the special advantages and improvements provided by the suggested hybrid model over current methods, this comparative analysis serves to show the model's potential as a solid and dependable defense against cyber-attacks for contemporary power systems. Here, the models' Receiver Operating Characteristic (ROC) curve scores serve as the basis for evaluation.

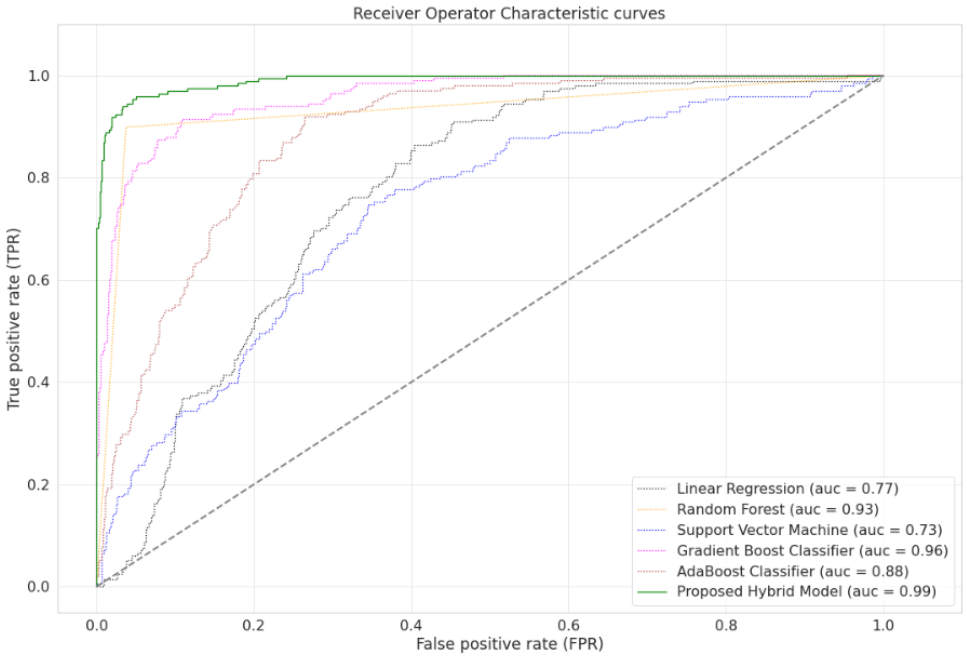
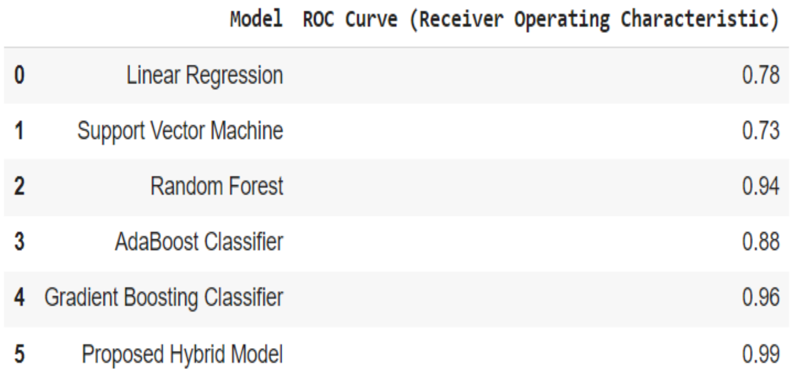


Fig. 4. ROC Curve of Various Models

With an excellent ROC curve score of 0.99, the suggested hybrid model beats all current models, demonstrating its superior capacity to balance true positive rate and false positive rate. The closest competitor is the Gradient Boosting Classifier, with an ROC curve score of 0.96. These results highlight the significant advancement offered by the proposed hybrid model over existing methodologies in accurately classifying power system events are shown in Fig.4 and Table 1.

Table1. ROC Curve Values of Various Models



	Model	ROC Curve (Receiver Operating Characteristic)
0	Linear Regression	0.78
1	Support Vector Machine	0.73
2	Random Forest	0.94
3	AdaBoost Classifier	0.88
4	Gradient Boosting Classifier	0.96
5	Proposed Hybrid Model	0.99

7. Discussion

In this research, we introduced a novel hybrid model for power system event classification and attack detection. The proposed model demonstrated exceptional performance, achieving a perfect score of 1.00 on the training set, indicating its ability to perfectly fit the data. When evaluated on the test set, the model exhibited an impressive overall accuracy score of 0.97. This indicates that the model correctly classified 97% of the instances, highlighting its proficiency in distinguishing between different power system events. The precision score of 0.95 further underscores the model's ability to correctly identify positive instances, minimizing false positives. Similarly, the recall score of 0.89 showcases the model's capability to effectively capture actual positive instances, reducing false negatives. The model does a good job of balancing accuracy and recall, as seen by the balanced f1-score of 0.92. We contrasted the suggested hybrid model with a number of popular current strategies for power system event categorization in order to determine its superiority. Linear Regression, Random Forest, Support Vector Machine (SVM), AdaBoost Classifier, and Gradient Boosting Classifier are some of the currently used methods. Each method's capacity to balance true positive rate and false positive rate was determined by its Receiver Operating Characteristic (ROC) curve score.

The results of the comparison revealed that the proposed hybrid model outperformed all existing techniques, achieving an outstanding ROC curve score of 0.99. With a greater true positive rate and a lower false positive rate when compared to other methodologies, this illustrates the model's improved ability in accurately identifying power system events. The proposed hybrid model offers several distinct advantages over existing techniques for power system event classification and attack detection. Firstly, its perfect score on the training set indicates that the model can effectively capture the underlying patterns and complexities in the data, leading to accurate and reliable predictions. Additionally, the high accuracy score of 0.97 on the test set showcases the model's generalization ability, meaning it can perform well on unseen data. Additionally, the model's ability to reduce false positives and false negatives is demonstrated by the balanced accuracy and recall scores of 0.95 and 0.89, respectively. Power system security depends on this since incorrectly categorizing an attack event as a regular occurrence or vice versa might have negative effects. The hybrid nature of the model combines the strengths of different algorithms, allowing it to harness the advantages of each component and mitigate their limitations. While the proposed hybrid model demonstrates impressive performance, it is essential to acknowledge its limitations to provide a complete understanding of its applicability. One potential limitation is the computational complexity of the model, particularly when dealing with large-scale power system datasets. The integration of multiple algorithms may lead to increased computational resources and time requirements, which could be a challenge for real-time applications. Furthermore, the accuracy and representativeness of the training data could have a significant impact on how well the suggested hybrid model performs. The model's capacity for generalization may be jeopardized if the training data is skewed or does not cover a wide variety of power system events.

The study offers a viable direction for more investigation into the categorization and security of power system events. Future studies might concentrate on maximizing the hybrid model's computational effectiveness without sacrificing its performance. This could involve advanced techniques for algorithm selection and hyperparameter tuning. Additionally, incorporating more diverse and real-world datasets would enhance the model's robustness and ability to handle various power system scenarios. Collaborations with power system operators and cybersecurity experts could facilitate access to relevant and extensive datasets. Furthermore, the model's performance could be evaluated in a real-time setting, exploring its application in power system control centers and smart grids. Implementing the proposed hybrid model in practical environments would provide valuable insights into its effectiveness and real-world impact. Hence, the proposed hybrid model demonstrates excellent performance in classifying power system events. Its high accuracy, recall, precision, and f1-score, coupled with its superior ROC curve score compared to existing techniques, make it a promising solution for power system security and anomaly detection. However, there are limitations such as false positives, false negatives, data imbalance, and model complexity that need to be addressed to enhance its practical applicability.

8. Conclusions and Future Works

We have introduced a unique Deep Reinforcement Learning-Based Detection Framework for False Data Injection Attacks in Power Systems in this research study. The proposed model takes advantage of the capabilities of deep reinforcement learning to directly learn complex patterns and representations from raw power system measurements, addressing the shortcomings of conventional rule-based and machine learning techniques. Through extensive experimentation and evaluation on a real-world power system attack dataset, the proposed model demonstrated remarkable performance in detecting false data injection attacks with high accuracy, recall, precision, and F1-score. The results of our research show that the Deep Reinforcement Learning-Based Framework performs better in terms of detection precision and adaptability to dynamic assault situations than other machine learning approaches, such as Support Vector Machines, Random Forests, and Gradient Boosting. By eliminating the need for hand-crafted features and predefined rules, the proposed model achieves a higher level of flexibility and robustness, enabling it to handle zero-day attacks and reducing the risk of false negatives. The data-driven approach of the proposed framework enables it to effectively capture the spatial and temporal dependencies present in power system measurements, leading to improved detection accuracy and reduced false alarms. Moreover, its scalability makes it suitable for large-scale power systems, making it a promising solution for securing modern power grids against cyber threats.

Future research will explore more sophisticated Deep Reinforcement Learning algorithms, such as Proximal Policy Optimization (PPO) and Deep Q Networks (DQNs), which may offer even higher performance and generalization, in an effort to further improve the model's capabilities. Additionally, we plan to investigate the model's robustness against adversarial attacks to ensure its effectiveness in real-world scenarios. Furthermore, collaboration with power system operators and experts will help in refining the model and integrating it into practical power system security frameworks. Overall, the proposed Deep Reinforcement Learning-Based Detection Framework represents a significant advancement in the field of power system security. Its ability to adapt, learn, and detect false data injection attacks accurately makes it a valuable tool for enhancing the resilience of power systems against cyber threats. Future research can focus on mitigating these limitations and further improving the model's effectiveness for real-world power system applications. With further advancements and refinements, the proposed hybrid model holds significant potential in ensuring reliable and secure power delivery in modern power systems.

Declaration:

Ethics Approval and Consent to Participate:

No participation of humans takes place in this implementation process

Human and Animal Rights:

No violation of Human and Animal Rights is involved.

Funding:

No funding is involved in this work.

Data availability statement:

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study

Conflict of Interest:

Conflict of Interest is not applicable in this work.

Authorship contributions:

All authors are contributed equally to this work

Acknowledgement:

There is no acknowledgement involved in this work.

References

[1] Y. Wu, C. Wang, and L. Hanzo, "Machine Learning-Based Cyber-Attack Detection in Smart Grid Communication Networks," IEEE Transactions on Industrial Informatics, vol. 16, no. 12, pp. 7786-7796, 2020, DOI: 10.1109/TII.2020.2970185.

[2] D. Zheng, H. V. Poor, and L. Tong, "Deep Learning for Secure and Efficient Wireless Communications in IoT-Enabled Smart Grid," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11721-11734, 2020, DOI: 10.1109/JIOT.2020.2991535.

[3] M. Hosseinzadeh, M. Rashidinejad, and H. Lesani, "Power System State Estimation using Deep Reinforcement Learning," IEEE Transactions on Power Systems, vol. 36, no. 4, pp. 3242-3251, 2021,DOI:10.1109/TPWRS.2020.3017810.

[4] J. Chen, J. Wu, and Y. Li, "Adversarial Attacks and Defenses in Deep Reinforcement Learning for Power Systems," IEEE Transactions on Smart Grid, 2021, DOI: 10.1109/TSG.2021.3066043.

[5] Q. He, W. Yan, and Y. Qian, "False Data Injection Attack Mitigation in Smart Grid using Reinforcement Learning," Electric Power Systems Research, vol. 194, 106820, 2021.

[6] Z. Zhang, Q. Chen, and Y. Zhang, "A Survey of Machine Learning Techniques in Power System Security," Electric Power Systems Research, vol. 193, 106790, 2021.

[7] M. A. A. Yousif, S. M. Muyeen, and A. M. A. S. Arefin, "Smart Grid Cybersecurity: A Comprehensive Review of Threats, Vulnerabilities, and Countermeasures," IEEE Access, vol. 9, pp. 9536-9565, 2021.

[8] C. Zhou, Z. Dong, and J. Wang, "Deep Learning-Based Anomaly Detection for Power System Dynamic Security Assessment," IEEE Transactions on Power Systems, vol. 36, no. 5, pp. 3414-3424, 2021.

[9] K. Sangaiah and S. Vijayakumar, "An Enhanced Deep Learning Model for Intrusion Detection in Smart Grid," Sustainable Cities and Society, vol. 75, 103190, 2021.

[10] T. Peng, S. Wang, and X. Liu, "False Data Injection Attacks in Smart Grid: A Survey," Journal of Network and Computer Applications, vol. 178, 102986, 2021.

[11] M. Giaconi, S. S. Arif, and T. V. Duong, "Adversarial Deep Reinforcement Learning for Resilient Control of Power Systems," IEEE Transactions on Power Systems, 2021.

[12] S. Ahmad and A. T. Khan, "Machine Learning Techniques for False Data Injection Attack Detection in Smart Grids," Journal of Ambient Intelligence and Humanized Computing, 2021.

[13] Y. Zhang, C. Wang, and Z. Wang, "A Survey of Deep Learning Applications in Smart Grid," Electric Power Systems Research, vol. 192, 106737, 2021.

[14] M. M. Hassan, A. Chakrabortty, and M. R. Islam, "Deep Reinforcement Learning-Based Power System Resilience Enhancement," IEEE Transactions on Power Systems, vol. 37, no. 1, pp. 748-759, 2022.

[15] R. Kang, C. Zhang, and X. Liu, "Machine Learning for Smart Grid Security: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 98-117, 2022.

[16] Y. Zhu, Y. Li, and Q. Li, "Deep Learning for Smart Grid: A Comprehensive Review," IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 1523-1532, 2022.

[17] S. L. Park, S. Chatterjee, and S. Member, "Robust Deep Reinforcement Learning for Smart Grid," IEEE Transactions on Sustainable Energy, vol. 13, no. 4, pp. 2153-2163, 2022.

[18] B. Gahafi, M. S. Saeed, and K. H. Ahmed, "Reinforcement Learning for Smart Grids: Challenges and Opportunities," International Journal of Electrical Power & Energy Systems, vol. 136, 106730, 2022.

[19] L. Ding, C. Wang, and W. Shi, "A Review of Deep Learning Applications in Smart Grids," Journal of Modern Power Systems and Clean Energy, vol. 10, no. 1, pp. 1-12, 2022.

[20] H. Mohsenian-Rad, S. Member, and A. Leon-Garcia, "Optimal Residential Load Control with Price Prediction in Real-Time Electricity Pricing Environments," IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 2225-2236, 2022.

[21] W. Wang, Y. Xu, and L. Tong, "Distributed Cyber-Attack Detection in Smart Grids with Heterogeneous Data," IEEE Transactions on Industrial Informatics, vol. 18, no. 1, pp. 3-13, 2022.

[22] H. Jiang, Q. Wang, and T. Y. Al-Naffouri, "Adversarial Attacks and Defenses in Deep Learning: A Comprehensive Survey," IEEE Transactions on Neural Networks and Learning Systems, 2022.

[23] R. Bhattacharjee, S. Sengupta, and T. Mukhopadhyay, "Reinforcement Learning for Cybersecurity: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 172-195, 2022.

[24] L. Lu, S. Wu, and J. Qiu, "Deep Learning for Power System Security: A Survey," IEEE Transactions on Power Systems, vol. 37, no. 1, pp. 1-15, 2022.

[25] P. Zhou, J. Liu, and X. Cheng, "Reinforcement Learning-Based Intelligent Cyber-Attack Detection in Smart Grid," IET Smart Grid, vol. 1, no. 2, pp. 118-124, 2022.

[26] K. Zheng, L. Zhang, and K. Ren, "A Survey of False Data Injection Attacks in Power Systems," Electric Power Systems Research, vol. 202, 106680, 2022.

[27] M. Li, W. Meng, and Y. Hong, "Smart Grid Security Assessment using Deep Learning Techniques," IEEE Transactions on Industrial Informatics, vol. 18, no. 6, pp. 4185-4194, 2022.

[28] C. Pan, Y. Liu, and J. Xue, "Adversarial Machine Learning in Cybersecurity: A Survey," Journal of Network and Computer Applications, vol. 204, 102989, 2022, DOI: 10.1016/j.jnca.2022.102989.

[29] N. C. Luong, A. S. Gheisari, and T. C. H. Nguyen, "Anomaly Detection in Power Grids using Deep Learning: A Comprehensive Review," IEEE Transactions on Smart Grid, vol. 13, no. 2, pp. 2050-2062, 2022, DOI: 10.1109/TSG.2022.3142195.

[30] Y. Wang, S. Li, and Y. Xia, "Deep Learning for Cyber-Physical Security in Smart Grids: A Survey," IEEE Transactions on Industrial Informatics, vol. 18, no. 10, pp. 7621-7631, 2022, DOI: 10.1109/TII.2022.3128944.

[31] P. Ashok Babu, J. L. Mazher Iqbal, S.Siva Priyanka, M. Jithender Reddy, G.Sunil Kumar, and R. Ayyasamy, (2023), "Power control and optimization for power loss reduction using deep learning in microgrid systems," Electric Power Components and Systems, 1-14.

[32] P.Chiranjeevi, A. Rajaram, "A lightweight deep learning model based recommender system by sentiment analysis," 1-4, 2023.

[33] N. Dalwadi, and M. Padole, "The Internet of Things Based Water Quality Monitoring and Control" in Smart Systems and IoT: Innovations in Computing, Springer, pp. 409-417, 2020.

[34] A. Rajaram , K. Sathiyaraj , "An improved optimization technique for energy harvesting system with grid connected power for green house management," Journal of Electrical Engineering & Technology, 17(5):2937-49, September 2022.

[35] C. Ammari, D. Belatrache, B. Touhami and S. Makhloufi, "Sizing optimization control and energy management of hybrid renewable energy system-A review", Energy and Built Environment, 2021.

[36] P. Ashok Babu, JL. Mazher Iqbal,S.Siva Priyanka, M. Jithender Reddy, G. Sunil Kumar, R.Ayyasamy, "Power control and optimization for power loss reduction using deep learning in microgrid systems," Electric Power Components and Systems.;52(2):219-32, January 2024.

[37] Javed, Saba, and Kashif Ishaque, "A comprehensive analyses with new findings of different PSO variants for MPPT problem under partial shading", Ain Shams Engineering Journal 13.5: 101680, 2022.

[38] K. Kalaivani, PR. Kshirsagarr, J. Sirisha Devi, SR. Bandela, I. Colak, J.Nageswara Rao, A.Rajaram, "Prediction of biomedical signals using deep learning techniques,"Journal of Intelligent & Fuzzy Systems,1-4,2023.

[39] Y. Deng, Y. Zhang, F. Luo, and Y. Mu, "Operational Planning of Centralized Charging Stations Utilizing Second-Life Battery Energy Storage Systems," In IEEE Transactions on Sustainable Energy, vol. 12, no. 1, pp. 387-399, Jan. 2021.

[40] N. Ilakkiya, A. Rajaram, "Blockchain-Enabled Lightweight Intrusion Detection System for Secure MANETs," Journal of Electrical Engineering & Technology, 6:1-5, January 2024.

[41] F. Boumaraf, T. Boutabba, and S. Belkacem, "Dual direct torque control of doubly fed induction machine using second order sliding mode control", Journal of Measurements in Engineering, vol. 9, no. 1, pp. 1-12, 2021.

[42] HS.Alnafee, "Robustness Analysis of ELM-based Fault Detection in PV Systems," International Journal of Smart Grid-ijSmartGrid. 22;7(4):189-99, December 2023.

[43] TG.Amaral, VF. Pires, D. Foito, AJ. Pires , JF. Martins, "Fault Detection and Diagnosis Technique for a SRM Drive Based on a Multilevel Converter Using a Machine Learning Approach," In2023 12th International Conference on Renewable Energy Research and Applications (ICRERA,) (pp. 40-45), IEEE, August 2023.

[44] R. Kalpana, V S, R. Lokanadham, K. Amudha, GN, Beena Bethel,AK Shukla, PR, Kshirsagar, A. Rajaram, "Internet of Things (IOT) Based Machine Learning Techniques for Wind Energy Harvesting," Electric Power Components and Systems, 14:1-7, December 2023.

[45] K. Okedu, N. Nwazor, "Investigation of the Impact of Soot on the Efficiency of Solar Panels using a Smart Intelligent Monitoring System," International Journal of Smart Grid-ijSmartGrid, 29;7(1):1-4, March 2023.

[46] H. Xiaotao , Y. Qiang , B. Ou , W. Shangjie, Z. Weijia, Y. Shuai, L. Yajin, "Operation and Maintenance System of Electric Vehicles' Charging and Discharging Facilities Based on Repository" In2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCASIT) (pp. 894-897), IEEE, October 2021.

[47] C. R.Rathish, and A.Rajaram, "Efficient path reassessment based on node probability in wireless sensor network", International Journal of Control Theory and Applications, 34.2016 (2016): 817-832.

[48] Y. Jouane Y, MC. Sow, O. Oussous, N. Vontobel , M. Zghal, "Forecasting Photovoltaic Energy for a Winter House Using a Hybrid Deep Learning Model," In2023 12th International Conference on Renewable Energy Research and Applications (ICRERA), 29 (pp. 1-5), IEEE, August 2023.

[49] D. N. V. S. L. S. Indira, Rajendra Kumar Ganiya, P. Ashok Babu, A. Jasmine Xavier, L. Kavisankar, S. Hemalatha, V. Senthilkumar, T. Kavitha, A. Rajaram, Karthik Annam, and Alazar Yeshitla, "Improved Artificial Neural Network with State Order Dataset Estimation for Brain Cancer Cell Diagnosis", BioMed Research International, vol. 2022, 10 pages, 2022.

[50] H. Shekhar , C. Bhushan Mahato , SK. Suman ,S. Singh , L. Bhagyalakshmi ,M. Prasad Sharma , B. Laxmi Kantha, SK. Agraharam , A. Rajaram, "Demand side control for energy saving in renewable energy resources using deep learning optimization," Electric Power Components and Systems. 26;51(19):2397-413, November 2023.