VOL. 11 NO. 9,
FEBRUARY, 2026
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

Hybrid ANN–DNN–LSTM Deep Learning Architecture for Botnet Detection in Smart Grid Cyber-Physical Systems

Agu Onyebueke Edward[1]; Saraso David Lami[2]; Madugu Jeremiah Omanga[3]; & Okimba P. E.[4]

[1]Department of Computer Science, Federal University Wukari, Taraba State, Nigeria. [2]Department of Computer Science, Kwararafa University Wukari, Taraba State, Nigeria. [3]Department of Computer Science, Taraba State University Jalingo, Taraba State, Nigeria. [4]Department of Computer Science, Taraba State Polytechnic Jalingo, Taraba State, Nigeria.

Corresponding Author: madugujeremiah4@gmail.com

DOI: https://doi.org/10.70382/ajsitr.v11i9.069

Abstract

Smart power grids are vital cyber-physical infrastructures that are more vulnerable to sophisticated cyberthreats, especially botnet-driven assaults, due to their growing reliance on IoT-enabled communication and control technology. These assaults have the potential to spread quickly across both physical and cyber levels, resulting in serious stability threats, operational interruptions, and cascade failures. Therefore, rapid and accurate intrusion detection is crucial since false negatives in power systems might have permanent physical repercussions. However, current intrusion detection methods based on standalone deep learning models frequently have poor handling of the temporal and nonlinear dependencies present in smart grid data, poor generalization, and high false-negative rates. To address these limitations, this study presents a hybrid ensemble deep learning framework that integrates Artificial Neural Networks (ANN), Deep Neural Networks (DNN), and Long Short-Term Memory (LSTM) models for enhanced botnet attack detection in smart grid cyber-physical environments. Through an ensemble-based decision technique, the framework makes use of the complementary characteristics of the component models, temporal learning, hierarchical feature extraction, and nonlinear pattern modeling. A benchmark smart grid dataset from the Kaggle Machine Learning Repository is used in a three-phase technique that includes data pretreatment, model integration, and performance evaluation. Experimental results demonstrate that the hybrid

ensemble significantly outperforms individual models upon evaluation, with a marked reduction in false negatives. These findings confirm the effectiveness of ensemble hybridization in improving detection reliability and resilience, positioning the proposed framework as a high-fidelity supervisory mechanism for securing smart grid cyber-physical systems against evolving botnet threats.

Keywords: Cyber-Physical Security, Hybrid Ensemble Deep Learning, Botnet Attack Detection, Smart Grid, ANN–DNN–LSTM Architecture.

INTRODUCTION

The modern power grid has evolved into a highly connected smart grid that combines state-of-the-art information and communication technologies (ICT) with physical power infrastructure to boost efficiency, reliability, and operational intelligence (Cavus, 2025). Smart grids function as complex cyber-physical systems (CPS) through elements including advanced metering infrastructure (AMI), distributed energy resources (DERs), Internet of Things (IoT) devices, and supervisory control and data acquisition (SCADA) systems (Khalaf *et al*., 2024). Real-time monitoring, automation, and bidirectional energy flow are made possible by this convergence, but it also greatly increases the cyberattack surface, leaving vital power infrastructure vulnerable to sophisticated and well-coordinated cyberthreats.

In smart grid environments, botnet breaches have become one of the most hazardous and disruptive types of cyber intrusion (Alomari *et al*., 2025). Attackers can perform coordinated load manipulation, fake data injection attacks (FDIAs), and distributed denial-of-service (DDoS) assaults by breaching a large number of IoT-enabled devices, including smart meters, electric car charging stations, and embedded controllers (Bhuiyan, 2025). Successful botnet assaults on smart grids, in contrast to standard IT networks, can have physical repercussions, such as equipment damage, cascade failures, grid instability, and widespread power outages. Because of this, prompt and precise identification of botnet activity is not just a cybersecurity requirement but also a basic requirement for preserving public safety and power system resilience (Nandini *et al*., 2024).

Because false negatives, malicious activity that goes unnoticed, can have serious and permanent effects, accurate intrusion detection is especially important in smart grid setups (Sahani *et al*., 2023). Adversaries may be able to continue operating within the system after a botnet assault is missed, progressively altering control signals or load patterns until a catastrophic collapse takes place. False negatives pose a direct danger to grid stability and dependability, but false positives may result in operational overhead (Reda *et al*., 2023). As a result, high detection sensitivity must be prioritized by intrusion detection systems (IDS) for smart grids while preserving resilience against intricate and dynamic assault patterns.

Due to their capacity to extract intricate, nonlinear patterns from massive datasets, deep learning-based methods have attracted a lot of interest recently for smart grid intrusion detection (Massaoudi *et al*., 2023). Models including long short-term memory (LSTM) networks, deep neural networks (DNN), and artificial neural networks (ANN) have shown encouraging results in detecting cyberattacks. However, when these models are applied alone, current research reveals significant limits. While LSTM-based methods are good at capturing sequential activity, they may be more computationally difficult and sensitive to data imbalance (Rithan *et al*., 2023; Kim & Nam, 2025). Standalone ANN and DNN models frequently have trouble simulating temporal dependence. More importantly, single-model approaches frequently exhibit elevated false-negative rates in dynamic cyber-physical environments, limiting their suitability for real-world smart grid protection (Zheng *et al*., 2022).

These limitations motivate the adoption of hybrid deep learning architectures, particularly ensemble-based models that integrate the complementary benefits of many learning paradigms. In this study, by combining ANN, DNN, and LSTM models into a single ensemble framework, the system may simultaneously employ various feature representations, temporal dynamics, and nonlinear decision restrictions. Such an ANN–DNN–LSTM ensemble hybrid model increases detection robustness by reducing the likelihood that complex or dynamic botnet patterns may evade all component models. Because avoiding false negatives is necessary to prevent cascade cyber-physical failures, this hybridization strategy is especially crucial for smart grid security. Therefore, this paper presents a hybrid ensemble deep learning framework composed of ANN, DNN, and LSTM models for enhanced botnet detection in smart grid cyber-physical environments. The ensemble architecture is designed to improve detection accuracy, robustness, and generalization while significantly reducing misclassification, particularly false negatives, compared to standalone deep learning models.

LITERATURE REVIEW

With a focus on botnet-driven and coordinated cyber-physical attacks, the literature review for this study is organized with a focus on earlier research that addressed cybersecurity issues in smart grid cyber-physical systems. It summarizes previous research to show how sophisticated detection and mitigation techniques beyond conventional security solutions have been spurred by growing interconnectedness, IoT proliferation, and legacy protocols. In order to improve threat detection accuracy and system resilience in smart grid contexts, the review is structured around hybrid and intelligent methodologies that combine domain expertise with data-driven learning.

Smart Grid Cyber-Physical Security Overview

In order to create complex cyber-physical systems (CPS) that span generation, transmission, distribution, control, and consumer interfaces, modern smart grids combine digital communication, sensing, and control technologies with conventional power infrastructure.

Through elements like SCADA systems, advanced metering infrastructure (AMI), and distributed energy resources (DERs), this interconnected architecture permits real-time monitoring and automation, but it also increases the attack surface across both cyber and physical layers (Zibaeirad *et al*., 2024; Mohan *et al*., 2024). Adversaries use weak authentication, unpatched IoT devices, and unsecured communication protocols like DNP3 and Modbus to execute botnet-driven assaults that can alter control signals, overburden network resources, or insert bogus data. These assaults may result in cascade failures, frequency/voltage instability, or operational interruptions (Maiti & Dey, 2024; Frontiers Energy Research, 2025). The growth of IoT endpoints, many of which are outside utility control, increases the likelihood of large-scale botnet exploitation, in which coordinated hacked devices carry out distributed denial-of-service (DDoS) attacks or load-altering operations that jeopardize grid stability (Lamisss *et al*., 2025). Legacy protocols with inadequate encryption and authentication raise the risks of lateral movement and covert attacks in SCADA and EMS networks, making detection and mitigation more difficult (MDPI, 2024).As a result, safeguarding smart grids requires security strategies that address vulnerabilities at both the cyber level (e.g., protocol misuse, network infiltration) and the physical level (e.g., manipulation of actuators and sensing devices), recognizing that cyber intrusions can rapidly translate into physical consequences. In order to improve the detection and analysis of cyber-physical threats in power systems, Presekal *et al.* (2023) developed a hybrid deep-learning-based attack graph model. They highlighted that conventional approaches have difficulty identifying complex industrial threats and showed that the hybrid model is more accurate in identifying multi-stage attacks in smart grid environments. By combining domain-specific structures with machine intelligence, their work was presented as addressing shortcomings in current anomaly and intrusion detection, suggesting enhanced resilience against cyber-physical attacks. The authors contended that such hybrid techniques can bridge gaps between model interpretability and detection performance in real-world grid security. In order to identify denial-of-service attacks by categorizing network traffic into benign and malicious classes, Sharma *et al.* (2023) presented a lightweight hybrid deep-learning model that combines CNN and Bidirectional LSTM. They said that in order to improve detection accuracy while preserving computational economy, the model made use of many convolutional and pooling layers with improved hyperparameters. Overall, Sharma et al. found that the suggested method improved IDS performance for smart healthcare CPS systems with limited resources. A hybrid deep learning system that combines CNN, GRU, and LSTM was proposed by Abbassy *et al*. (2025) to enhance cyber threat categorization in CPS scenarios. They clarified that the CNN component obtains spatial information from preprocessed data, GRU learns temporal features, and LSTM classifies different abnormalities and attacks. They suggested that this method might exceed current approaches in terms of accuracy, sensitivity, and specificity. The authors contended that their hybrid model outperforms conventional intrusion detection methods in addressing both temporal and geographical components of data. They said that in order to show the potential benefits of their

approach, it was compared to previous research. Using phasor measurement unit (PMU) data for anomaly detection, Bitirgen and Filik (2023) created a hybrid deep learning model that combines convolutional neural networks and long short-term memory (CNN-LSTM) optimized with particle swarm optimization (PSO) to differentiate between physical disruptions and false data injection attacks in smart grid systems. They claimed that their suggested PSO-CNN-LSTM model beat comparator models in terms of accuracy and efficacy when compared to cutting-edge deep learning architectures. Additionally, they pointed out that the improved model might offer trustworthy decision assistance for preserving safe and stable grid operations. Bitirgen and Filik stressed that strengthening the resilience of smart grid security systems against malevolent assaults requires improved anomaly detection procedures. They concluded that their hybrid approach shows promise as a component of more robust cyber-physical protection strategies for critical infrastructure.

According to Ruben *et al*. (2020), as smart grids develop, their real-time monitoring systems are more susceptible to cyberattacks, particularly bogus data injection assaults, which they referred to as "bad data." According to their findings, traditional detection techniques that rely only on statistical tests and physics-model weighted least-squares estimators are intrinsically constrained by linear approximations and modeling mistakes. In order to increase robustness, Ruben et al. suggested a hybrid approach that combines physics-based detection with data-driven anomaly detection using data fusion. They claimed that in order to improve overall detection performance, this fusion takes into account the confidence levels of various detectors at both the global and local levels. They suggested improved detection capabilities against coordinated cyber-physical threats after validating their method on the IEEE 118-bus test system. In order to improve intrusion detection in cyber-physical systems, Arumugam *et al*. (2024) developed a hybrid deep architecture that combines deep learning with optimization approaches to increase system robustness and classification accuracy. They clarified that their optimization-based approach could more effectively adjust to these difficulties while lowering false alarms, while conventional intrusion detection systems frequently had trouble with asymmetric and changing threats. The authors emphasized increases in detection rates and computing efficiency, noting that experimental findings demonstrated higher performance when compared to baseline approaches. Additionally, they emphasized how combining optimization techniques with deep neural networks aided in striking a balance between feature learning exploration and exploitation. Lastly, Arumugam *et al.* proposed that real-world cyber-security applications requiring complex system settings might successfully adopt this hybrid method. Garg *et al.* (2022) developed a Dynamic Hybrid Secured Encryption (DHSE) method that combines AES, IBE, and ABE to improve encryption efficiency and classify data according to sensitivity. They claimed that by cutting down on both encryption and decryption times, the DHSE performed better than current individual encryption techniques. They stressed that as compared to traditional methods, their results showed better performance and secrecy. They came to the conclusion that the suggested framework is a good fit for safe CPS-IoT settings in smart businesses. A deep hybrid model combining a gated recurrent unit, long

short-term memory architecture, and one-dimensional convolutional neural network was proposed by Alguliyev *et al.* (2021). The SPOCU activation function and a modified Adam optimizer were incorporated into their design to enhance performance, according to the authors. Experimental tests on two benchmark datasets demonstrated the model's superior classification accuracy when compared to existing machine learning techniques, indicating its efficacy in identifying anomalies and attacks within crucial cyber-physical environments. Gulzar and Mustafa (2024) developed a hybrid mode that incorporates logistic regression (LR), incremental principal component analysis (IPCA), and k-nearest neighbor (KNN) to increase attack detection accuracy. The authors report that experiments on the Secure Water Treatment (SWaT) dataset demonstrated increased performance, particularly with KNN achieving good accuracy, recall, and F1-score. They note that combining dimensionality reduction with machine learning techniques may significantly improve CPS threat detection. Finally, Gulzar and Mustafa argue that their approach offers a feasible path for more research on intelligent and flexible cybersecurity systems.

To adjust classifier weights, Sagu *et al*. (2025) used a hybrid framework that combined deep learning models, a Deep Belief Network and a Convolutional Neural Network, with a brand-new optimization technique they called Seagull Adapted Elephant Herding Optimization (SAEHO). The authors claim that this "hybrid classifier + SAEHO" strategy consistently beat traditional detection techniques across benchmark datasets when assessed using a variety of measures, including accuracy, precision, sensitivity, and specificity. Additionally, they emphasized that their system improved the detection of cyberattacks in IoT-enabled CPSs more robustly than previous models by combining deep learning with optimization. The authors came to the conclusion that their hybrid algorithm is a potential development for protecting smart settings from constantly changing cyberthreats. According to Sakhnini *et al*. (2021), the results they obtained on a smart grid dataset from Oak Ridge National Laboratories demonstrated better threat classification and localization performance when compared to conventional classifiers, indicating enhanced cybersecurity mitigation support. An intelligent ensemble machine-learning model that can identify and localize physical-layer attacks in smart grid communications was developed by Sakhnini *et al.*

While previous research has shown the potential of deep and hybrid learning approaches for cyber-physical security in smart grids, there is still a crucial gap in successfully resolving false negatives, which pose serious hazards to grid stability when botnet activity goes unnoticed. ANN, DNN, and LSTM are examples of standalone deep learning models that have significant drawbacks, such as poor temporal modeling, susceptibility to data imbalance, and high false-negative rates in dynamic cyber-physical contexts. Although a number of hybrid strategies have been put forth, ensemble-based hybrid architectures that concurrently use complementary learning paradigms to improve detection sensitivity and resilience have received less attention. This gap underscores the need for a unified ANN–DNN–LSTM ensemble framework capable of capturing nonlinear, spatial, and temporal attack

characteristics, thereby reducing misclassification and strengthening botnet detection in smart grid cyber-physical systems.

METHODOLOGY

In order to detect botnets in smart grid cyber-physical settings, this study adopts a three-phase methodological approach based on a hybrid ensemble deep learning architecture. To guarantee excellent data quality and dependable model learning, a labeled smart-grid traffic dataset from the Kaggle Machine Learning Repository is first thoroughly preprocessed using data cleaning, normalization, and class balancing. To maintain statistical consistency and avoid sample bias, the improved dataset is then divided using a 70:30 training–validation split. In order to capture the nonlinear interactions, hierarchical feature representations, and temporal dependencies prevalent in smart grid communication traffic, three complementary deep learning models, ANN, DNN, and LSTM, were implemented individually after which the three model were combined into a single hybrid ensemble framework that aims to minimize misclassification, especially false negatives linked to intricate botnet activities, by utilizing their combined strengths. The last stage verifies the ensemble model's robustness in a simulated smart grid environment and assesses it against its standalone counterparts using common performance metrics, such as accuracy, precision, recall, and F1-score, proving its efficacy for real-world cyber-physical security deployment. Figure 1 presents the methodology adopted for this study.

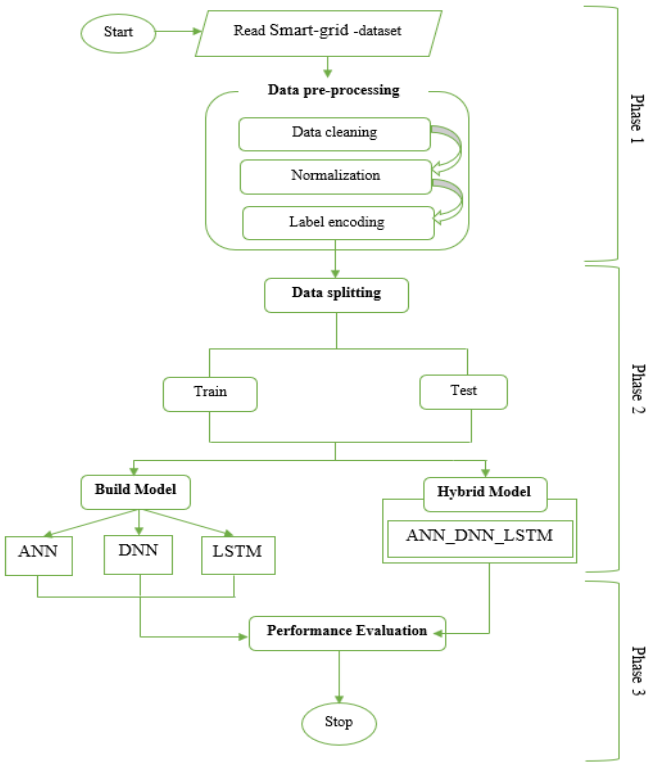


Figure 1: Research Methodology

Hybrid Ensemble Model

By utilizing the complementary characteristics of several deep learning architectures, the Hybrid Ensemble Model presented in this paper aims to improve botnet attack detection in smart grid cyber-physical systems. The framework combines ANN, DNN, and LSTM networks into a single ensemble-based detection system instead of depending on a single model. The diverse and dynamic character of smart grid data, which show nonlinear feature correlations, high dimensionality, and significant temporal dependencies, is what drove this design decision. The hybrid ensemble model enhances robustness, generalization, and resilience against complex and dynamic botnet threats by integrating several learning paradigms. The very same preprocessed smart grid traffic data is analyzed independently by each component model in the ensemble. In order to effectively distinguish between benign and malicious traffic patterns, the ANN component focuses on collecting nonlinear relationships among statistical and protocol-level data. In order to learn hierarchical and abstract feature representations, which are especially helpful for spotting intricate attack signatures that might not be seen at shallow levels, the DNN component uses a number of hidden layers. The system can identify covert and slowly changing botnet activity over time since the LSTM component models sequential behaviors and long-term temporal relationships. At the decision level, an ensemble learning technique is used to integrate the ANN, DNN, and LSTM models. The final classification decision is obtained by aggregating the probabilistic predictions that each model generates on the probability of botnet activity using a weighted fusion process. Because an attack overlooked by one model can still be detected by other models in the ensemble, this ensemble-based hybridization greatly lowers the probability of false negatives. Because undetected assaults may quickly grow into physical disturbances in smart grid scenarios, the hybrid model provides better detection sensitivity and reliability than solo deep learning systems. Therefore, the Hybrid Ensemble Model offers a scalable and flexible intrusion detection approach designed for cyber-physical systems in smart grids. The ensemble framework solves important drawbacks of single-model techniques and provides a more reliable protection against botnet-driven cyber-physical threats by concurrently using nonlinear feature learning, deep representation extraction, and temporal sequence modeling.

Mathematical Formulation of the Ensemble Decision Rule

Let the preprocessed input feature vector be represented as

$$x \in \mathrm{R}^n \quad (1)$$

where n denotes the number of selected features extracted from smart grid traffic data.

Each deep learning model independently computes a prediction score or class probability for the input sample x:

$$y_{ANN} = f_{ANN}(x) \quad (2)$$

$$y_{DNN} = f_{DNN}(x) \quad (3)$$

$$y_{LSTM} = f_{LSTM}(x) \quad (4)$$

Where $f_{ANN}(\cdot), f_{DNN}(\cdot), and f_{LSTM}(\cdot)$ denote the learned decision functions of the ANN, DNN, and LSTM models, respectively. Each output $y_i \in [0,1]$ represents the probability of a botnet attack.

The ensemble decision function combines these outputs using a weighted aggregation strategy:

$$y_{ensemble} = \sum_{i=1}^{3} w_i \cdot y_i \quad (5)$$

This is subject to:

$$\sum_{i=1}^{3} w_i = 1, w_i \geq 0 \quad (6)$$

where w_i represents the weight assigned to each model based on its validation performance. The final classification decision $\hat{y}_i$ is obtained using a threshold-based rule:

$$\hat{y} \begin{cases} 1, & if\ y_{ensemble} \geq r \\ 0, & otherwise \end{cases} \quad (7)$$

where $\hat{y} = 1$ indicates botnet activity, $\hat{y} = 0$ denotes normal behavior, and r is a predefined decision threshold (typically $r = 0.5$).

This ensemble formulation ensures that malicious activities overlooked by any single model can still be detected through collective decision-making, thereby significantly reducing false negatives and improving the reliability of intrusion detection in smart grid cyber-physical systems.

Algorithm: Hybrid Ensemble Deep Learning–Based Botnet Detection

Input:

Smart grid traffic dataset D

Decision threshold τ

Model weights w_{ANN}, w_{DNN}, w_{LSTM}

Output:

Final classification label $\hat{y}$(Normal or Botnet)

Begin

// Phase 1: Data Preprocessing

Clean dataset D by handling missing values and outliers

Normalize and standardize features in D

Extract relevant features for intrusion detection

Split D into training, validation, and test sets

// Phase 2: Model Training

Train ANN model using training set

Train DNN model using training set

Train LSTM model using training set

Optimize hyperparameters for each model using validation set

// Phase 3: Ensemble-Based Detection
For *each test sample x in test set* ***do***
Compute ANN prediction:
$y_{ANN} \leftarrow f_{ANN}(x)$
Compute DNN prediction:
$y_{DNN} \leftarrow f_{DNN}(x)$
Compute LSTM prediction:
$y_{LSTM} \leftarrow f_{LSTM}(x)$

// Decision-Level Ensemble Fusion
$y_{ensemble} \leftarrow (w_{ANN} \times y_{ANN}) + (w_{DNN} \times y_{DNN}) + (w_{LSTM} \times y_{LSTM})$

// Final Classification Decision
If $y_{ensemble} \geq \tau$ ***then***
$\hat{y} \leftarrow$ *Botnet Attack*
Else
$\hat{y} \leftarrow$ *Normal Traffic*
End If
End For

// Phase 4: Performance Evaluation
Evaluate ensemble performance using Accuracy, Precision, Recall, and F1-score
End

Model Hyperparameter Configuration and Training Strategy

To ensure reproducibility and transparency of the experimental setup, the hyperparameters used for training the ANN, DNN, and LSTM models were carefully defined and kept consistent across experiments where applicable. All models were implemented using the TensorFlow/Keras framework and trained using the Adam optimizer with a learning rate of 0.001. Binary classification was performed using the binary cross-entropy loss function, while accuracy was used as the primary evaluation metric. Each model was trained for a maximum of 100 epochs with a batch size of 8.

To prevent overfitting and improve generalization, an early stopping mechanism is employed, monitoring validation loss with a patience value of 10 epochs. Additionally, a ReduceLROnPlateau strategy is applied, reducing the learning rate by a factor of 0.5 if the validation loss failed to improve for 5 epochs, with a minimum learning rate of 0.0001.

The ANN model consists of three hidden layers with 64, 32, and 16 neurons, respectively, all using the ReLU activation function. Dropout regularization was applied with rates of 0.3 and 0.2 in the first two hidden layers to mitigate overfitting. The output layer used a sigmoid activation function with a single neuron to perform binary classification.

The DNN architecture consists of four fully connected hidden layers containing 128, 64, 32, and 16 neurons. Each hidden layer employed the ReLU activation function, while the output layer used a sigmoid function. To improve training stability and convergence, batch normalization was applied after the first two hidden layers. Dropout regularization was also incorporated with rates of 0.4, 0.3, 0.2, and 0.1 across successive layers.

The LSTM model captures temporal dependencies within smart grid traffic data. The architecture consisted of two stacked LSTM layers with 50 and 25 units, respectively. The first LSTM layer returned sequences to enable hierarchical temporal feature learning, while the second layer returned the final sequence output. A fully connected dense layer with 16 neurons and ReLU activation was used before the output layer. Dropout rates of 0.3, 0.3, and 0.2 were applied to improve model generalization. The final output layer used a sigmoid activation function for binary classification.

Class Balancing Technique

The dataset exhibited moderate class imbalance between normal and botnet-induced states. To mitigate potential bias toward the majority class, a class-weighting strategy was applied during model training. Class weights were computed based on the inverse frequency of each class and incorporated into the loss function during training. This approach ensures that misclassification of minority-class samples (botnet attacks) receives higher penalty during optimization, thereby improving detection sensitivity and reducing false negatives.

Ensemble Weight Determination

The ensemble decision mechanism combines the probabilistic outputs of the ANN, DNN, and LSTM models using a weighted aggregation strategy. The weights assigned to each model were determined based on their validation performance during training. Specifically, the F1-score obtained on the validation set was used as the primary criterion for weight assignment, as it balances precision and recall in security-sensitive applications. Models with higher validation F1-scores were assigned proportionally larger weights in the ensemble decision function. The final ensemble prediction was obtained through a weighted sum of the individual model probabilities followed by threshold-based classification. The detailed hyperparameter configuration of the ANN, DNN, and LSTM models used in this study is summarized in Table1.

Table 1: Summary of Model Hyperparameters

Category	Parameter	ANN	DNN	LSTM
Training Configuration	Optimizer	Adam	Adam	Adam
	Learning Rate	0.001	0.001	0.001
	Loss Function	Binary Cross-Entropy	Binary Cross-Entropy	Binary Cross-Entropy
	Evaluation Metric	Accuracy	Accuracy	Accuracy

Category	Parameter	ANN	DNN	LSTM
	Epochs	100	100	100
	Batch Size	8	8	8
	Early Stopping Monitor	Validation Loss	Validation Loss	Validation Loss
	Early Stopping Patience	10	10	10
	Reduce LR Factor	0.5	0.5	0.5
	Reduce LR Patience	5	5	5
	Minimum Learning Rate	0.0001	0.0001	0.0001
Network Architecture	Hidden Layers	3	4	2 LSTM + Dense
	Layer Units	64, 32, 16	128, 64, 32, 16	50, 25
	Dense Layer Units	—	—	16
	Activation Function	ReLU	ReLU	ReLU (Dense)
	Output Activation	Sigmoid	Sigmoid	Sigmoid
Regularization	Dropout Rates	0.3, 0.2	0.4, 0.3, 0.2, 0.1	0.3, 0.3, 0.2
	Batch Normalization	No	Yes (first two layers)	No
Sequence Configuration	Return Sequences	—	—	True (Layer 1), False (Layer 2)
	Input Shape	—	—	(timesteps = features, features = 1)

Performance Evaluation Metrics

Standard classification performance measures are used to critically assess the effectiveness of the hybrid ensemble deep learning framework for botnet identification in smart grid cyber-physical settings. For security-sensitive smart grid applications, these metrics offer a thorough assessment of detection accuracy, resilience, and dependability. Let TP stand for true positives (botnet attacks accurately detected), TN for true negatives (normal traffic correctly categorized), FP for false positives (normal traffic incorrectly classified as an attack), and FN for false negatives (botnet attacks that go unnoticed).

Accuracy measures the overall correctness of the detection system and is defined as:

$$\boldsymbol{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

Accuracy reflects the general effectiveness of the hybrid ensemble model in distinguishing between benign and malicious smart grid traffic, although it is interpreted cautiously due to possible class imbalance.

Precision quantifies the reliability of attack predictions and is expressed as:

$$\boldsymbol{Precision} = \frac{TP}{TP + FP} \quad (9)$$

Precision indicates the proportion of detected attacks that are truly malicious. High precision in this study implies reduced false alarms, thereby minimizing unnecessary operational interventions in smart grid control environments.

Recall, also known as sensitivity or detection rate, is defined as:

$$\boldsymbol{Recall} = \frac{TP}{TP + FN} \quad (10)$$

Recall is a critical metric in this study, as it measures the model's ability to correctly identify actual botnet attacks. A high recall value corresponds to a low false-negative rate, which is essential for preventing undetected intrusions that could escalate into physical grid failures.

F1-score provides a balanced evaluation of detection performance by combining precision and recall through their harmonic mean:

$$\mathbf{F1}_{\boldsymbol{-Score}} = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (11)$$

F1-score reflects the hybrid ensemble model's ability to achieve high detection sensitivity while maintaining reliable classification decisions.

RESULTS AND DISCUSSION

The experimental findings from assessing the hybrid ensemble deep learning framework for botnet identification in smart grid cyber-physical settings are presented and discussed in this part. The discussion highlights the efficacy of the hybrid strategy in improving smart grid security by emphasizing detection accuracy, resilience, and the decrease of false negatives.

Experimental Setup

This study's experimental setting was designed to facilitate the building, training, and assessment of hybrid ensemble models for identifying abnormalities caused by botnets in a smart grid cyber-physical environment. A 64-bit Windows system with an Intel® CoreTM i5-3630QM processor running at 2.40 GHz and 4 GB RAM was used for all simulations. This system offered sufficient computing power for data preprocessing, model training, and performance assessment. The Anaconda distribution with Python 3.8, chosen for its resilience in machine learning research and smooth interaction with scientific computing libraries, was used to create the model. The TensorFlow/Keras framework was used to build and train the hybrid ANN_DNN_LSTM model, while Pandas, NumPy, and Scikit-learn were used for data preparation and feature handling tasks. Matplotlib-generated graphics were used to assess model behaviors and experimental outcomes. The reproducibility, consistency, and dependability of the findings presented in this study were guaranteed by this clearly specified experimental setting.

Dataset Description and Visualization

The smart-grid cyber-physical dataset employed in this study comprises 60,000 records with 14 features, including 13 continuous numerical variables, torque parameters (tau1–tau4),

power measurements (p1–p4), generator indicators (g1–g4), and the stability index (stab), and a single categorical target label (stabf) representing normal versus botnet-induced unstable states. An initial data integrity assessment confirmed the absence of missing values, demonstrating a high-quality dataset suitable for immediate analytical processing. Visualization of the target label revealed class imbalance between normal and anomalous states, an important consideration for model design and evaluation. Exploratory feature analyses indicated clear correlations and structural dependencies among process variables, while Principal Component Analysis (PCA) showed that the leading components captured a substantial portion of variance, supporting the feasibility of dimensionality reduction for improved interpretability.

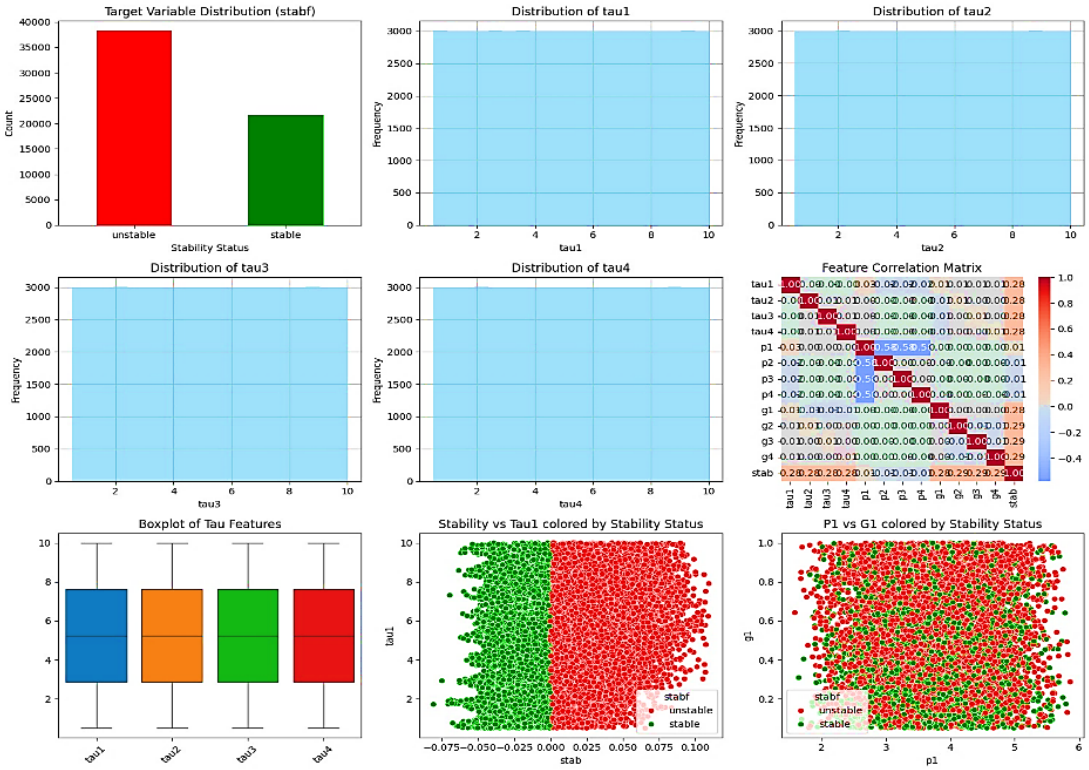


Figure 2: Visualization of Cleansed Dataset

Figure 2 shows the distribution and consistency of both numerical and categorical characteristics after cleaning, normalization, and label encoding, verifying continuous value ranges, logical patterns, and appropriate management of class imbalance. The quality and structure of the dataset are generally validated by these descriptive and visual assessments, which offer a strong basis for training the ANN–DNN–LSTM hybrid ensemble model for reliable botnet detection in smart-grid cyber-physical systems.

Hybrid Model's Confusion Matrix

The hybrid ensemble model's confusion matrix, which provides a thorough analysis of its classification performance in comparison to standalone designs, is shown in Figure 3.

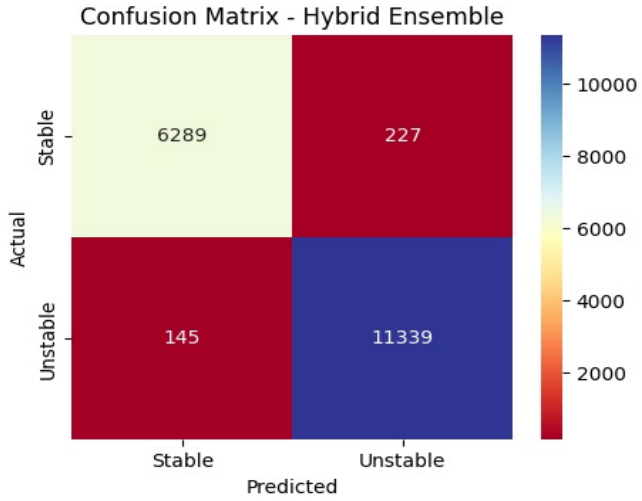


Figure 3: Hybrid Model Confusion Matrix

Strong diagonal dominance in the matrix indicates a significant decrease in false positives and false negatives as well as the improved discriminative power of the model. This enhancement demonstrates the synergistic impact of combining complementary learning capabilities, such as the hierarchical representation learning of DNN, the temporal modeling of LSTM, and the nonlinear feature mapping of ANN. The hybrid ensemble performs better than individual state-of-the-art models in precisely identifying botnet-induced anomalies and capturing minute changes in operational states, as seen by the low misclassification rates. Collectively, these findings confirm that the hybrid framework functions as a robust and reliable supervisory tool, capable of improving the sensitivity, accuracy, and resilience of smart grid intrusion detection systems.

Hybrid Model's Result

The hybrid model, developed using an ensemble approach, synergistically integrates the complementary capabilities of deep feedforward and recurrent neural networks to improve detection accuracy in the smart-grid cyber-physical environment. This model demonstrated a significant enhancement in performance across all key evaluation metrics, accuracy, precision, recall, and F1-score. The observed increase demonstrates the model's ability to concurrently capture temporal dependencies via the LSTM component and static nonlinear feature interactions through the feedforward network. This dual capacity successfully addresses the shortcomings found in the single-model techniques by significantly reducing both false positives and false negatives. Furthermore, a more accurate description of dynamic behaviors in smart-grid operations is made possible by the hybrid architecture's increased sensitivity to

minute temporal patterns indicative of botnet activity. The hybrid model provides a reliable and broadly applicable detection framework appropriate for real-time monitoring of cyber-physical abnormalities by utilizing many representational paradigms.

Table 2: Hybrid Model's Result

Model	Accuracy	Precision	Recall	F1-Score
Hybrid (ANN_DNN_LSTM)	0.9793	0.9804	0.9874	0.9839

The assessment findings, as shown in Table 2, validate the hybrid model's efficacy as a high-performance supervisory tool, fulfilling the study's goal of developing a trustworthy cyber-security supervisor for contemporary smart-grid systems.

Comparative Performance of Standalone and Hybrid Models

To empirically validate the performance advantage of the proposed hybrid architecture, a comparative evaluation was conducted between the standalone deep learning models (ANN, DNN, and LSTM) and the proposed hybrid ensemble model. Each model was trained and evaluated under the same experimental conditions using the preprocessed smart grid cyber-physical dataset. The comparison results are presented in Table 3.

Table 3: Model Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score
ANN	0.9593	0.9515	0.9864	0.9687
DNN	0.9638	0.9604	0.9838	0.9720
LSTM	0.9749	0.9834	0.9772	0.9803
Hybrid (ANN–DNN–LSTM)	0.9793	0.9804	0.9874	0.9839

The comparative results indicate that all standalone models demonstrate strong capability in detecting botnet activities within the smart grid cyber-physical dataset. The ANN model achieved an accuracy of 95.93%, effectively capturing nonlinear relationships among operational features, although its lower precision suggests a relatively higher false-positive rate. The DNN model improved performance with 96.38% accuracy and a higher F1-score, reflecting the advantage of deeper hierarchical feature representation in identifying complex intrusion patterns. Among the individual models, LSTM performed best, achieving 97.49% accuracy and an F1-score of 0.9803, largely due to its ability to model temporal dependencies and sequential patterns in smart grid communication data. However, the proposed hybrid ANN–DNN–LSTM ensemble model outperformed all standalone models, achieving the highest accuracy (97.93%), recall (98.74%), and F1-score (0.9839**)**. This improved performance results from integrating the complementary strengths of ANN for nonlinear feature learning, DNN for deep representation extraction, and LSTM for temporal sequence modeling. Through weighted ensemble fusion, the hybrid framework reduces misclassification, particularly false negatives, by allowing attacks missed by one model to be

detected by others, thereby enhancing detection robustness and reliability. Overall, the results empirically confirm that the ANN–DNN–LSTM hybrid ensemble architecture provides superior and more resilient botnet detection performance compared to standalone deep learning models in smart grid cyber-physical environments.

Performance Comparison Bar Chart

The comparative performance visualization in Figure 4 further highlights the superiority of the proposed hybrid ensemble model over the standalone architectures. The hybrid ANN–DNN–LSTM model consistently achieves the highest scores across most evaluation metrics, particularly in accuracy, recall, and F1-score. While the LSTM model performs competitively due to its ability to capture temporal dependencies in smart grid traffic data, the hybrid model benefits from integrating the complementary strengths of ANN, DNN, and LSTM within a unified ensemble framework. This combined learning capability enables improved detection sensitivity and reduced misclassification, reinforcing the effectiveness of the proposed hybrid approach for securing smart grid cyber-physical systems against botnet attacks.

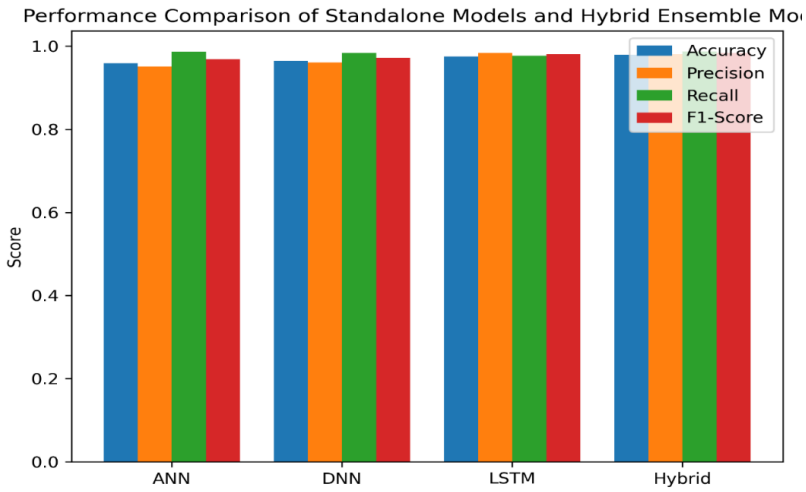


Figure 4: Performance comparison of standalone models (ANN, DNN, LSTM) and the proposed hybrid ANN–DNN–LSTM ensemble model

CONCLUSION

This study presents a robust hybrid ensemble deep learning framework that integrates ANN, DNN, and LSTM models to enhance botnet attack detection in smart grid cyber-physical systems. By leveraging the complementary capabilities of nonlinear feature learning, deep hierarchical representation, and temporal sequence modeling, the proposed framework addresses key limitations of standalone deep learning approaches, particularly their vulnerability to false negatives in dynamic smart grid environments. Experimental results demonstrate that the hybrid ANN–DNN–LSTM model achieves superior performance compared to individual models, attaining 97.93% accuracy, 98.74% recall, and an F1-score of

0.9839. In comparison with standalone baselines, the hybrid framework improves accuracy by approximately 2.0% over ANN, 1.55% over DNN, and 0.44% over LSTM, while also achieving the highest recall, which is critical for minimizing undetected botnet attacks in cyber-physical infrastructures. These improvements highlight the effectiveness of ensemble hybridization in enhancing detection reliability and reducing misclassification in smart grid security monitoring. Overall, the proposed architecture provides a robust supervisory mechanism capable of strengthening the resilience of smart grid cyber-physical systems against evolving botnet-driven cyber threats.

Future Direction

Even with these promising findings, there are still a number of areas that may be investigated further. First, the hybrid ensemble framework's practical applicability and scalability would be further demonstrated by real-time deployment and validation in live or hardware-in-the-loop smart grid systems. Second, in order to dynamically modify model contributions in response to changing assault patterns, future research may investigate adaptive ensemble weighting techniques and online learning methods. Additionally, by offering interpretable insights into detection choices, using explainable AI (XAI) approaches might increase model transparency and operator confidence.

REFERENCES

Abbassy, M. M., Satya Sai Kumar, A., Ead, W. M., Mohamed Aboalndr, A. A., Alsheref, F. K., Abdalla, M., & Shivani, A. (2025). Hybrid deep learning framework for detection of anomalies in cyber-physical systems. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-025-02633-7

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2021). Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems. *Neural Computing and Applications,* 33(16), 10211–10226. https://doi.org/10.1007/s00521-021-05785-2

Alomari, M. A., Al-Andoli, M. N., Ghaleb, M., Thabit, R., Alkawsi, G., Alsayaydeh, J. A. J., & Gaid, A. S. (2025). Security of smart grid: cybersecurity issues, potential cyberattacks, major incidents, and future directions. *Energies*, *18*(1), 141.

Arumugam, S. R., Paul, P. M., Issac, B. J. J., & Ananth, J. P. (2024). Hybrid deep architecture for intrusion detection in cyber-physical system: An optimization-based approach. *International Journal of Adaptive Control and Signal Processing, 38*(9), 3016–3039. https://doi.org/10.1002/acs.3855

Bhuiyan, T. (2025). AI in Smart Grid Cybersecurity: A Systematic Review of Machine Learning and Deep Learning Approaches against False Data Injection and Other Emerging Attacks. *Journal of Computer Science and Technology Studies*, *7*(8), 1207-1295.

Bitirgen, K., & Filik, Ü. B. (2023). A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. *International Journal of Critical Infrastructure Protection, 40*, Article 100582. https://doi.org/10.1016/j.ijcip.2022.100582

Cavus, M. (2025). Advancing Power Systems with Renewable Energy and Intelligent Technologies: A Comprehensive Review on Grid Transformation and Integration. *Electronics*, *14*(6), 1159.

Frontiers Energy Research. (2025). Exploring the emerging role of large language models in smart grid cybersecurity: A survey of attacks, detection mechanisms, and mitigation strategies. *Frontiers in Energy Research.* https://www.frontiersin.org/journals/energy-research/articles/10.3389/fenrg.2025.1531655

Garg, D., Rani, S., Herencsar, N., Verma, S., Wozniak, M., & Ijaz, M. F. (2022). Hybrid technique for cyber-physical security in cloud-based smart industries. Sensors, 22(12), 4630. https://doi.org/10.3390/s22124630

Gulzar, Q., & Mustafa, K. (2024). Hybrid cyber-attack detection model on cyber-physical systems using machine learning techniques. In A. Swaroop, Z. Polkowski, S. D. Correia, & B. Virdee (Eds.), *Proceedings of Data Analytics and Management: ICDAM 2023* (pp. 197–214). Springer. https://doi.org/10.1007/978-981-99-6547-2_16

Khalaf, M., Ayad, A., Tushar, M. H. K., Kassouf, M., & Kundur, D. (2024). A survey on cyber-physical security of active distribution networks in smart grids. *IEEe Access*, *12*, 29414-29444.

Kim, B. J., & Nam, I. W. (2025). A Review of Hybrid LSTM Models in Smart Cities. *Processes*, *13*(7), 2298.

Lamisss, S. D., Edward, A. O., & Omanga, M. J. (2025). A review of cyber-physical security strategies in smart power grids: Deep learning and hybrid approaches for botnet attack detection and mitigation. Global Scientific Journal, 13**(11).** https://www.globalscientificjournal.com/researchpaper/A_REVIEW_OF_CYBER_PHYSICAL_SECURITY_STRATEGIES_IN_SMART_POWER_GRIDS_DEEP_LEARNING_AND_HYBRID_APPROACHES_FOR_BOTNET_ATTACK_DETECTION_AND_MITIGATION.pdf

Maiti, S., & Dey, S. (2024). Smart grid security: A verified deep reinforcement learning framework to counter cyber-physical attacks.

Massaoudi, M., Abu-Rub, H., Refaat, S. S., Chihi, I., & Oueslati, F. S. (2021). Deep learning in smart grid technology: A review of recent advancements and future prospects. *IEEE Access*, *9*, 54558-54578.

MDPI. (2024). Security of smart grid: Cybersecurity issues, potential cyberattacks, major incidents, and future directions. Energies, 18(1).

Mohan, S. N., Ravikumar, G., & Govindarasu, M. (2024). Distributed intrusion detection system using semantic-based rules for SCADA in smart grid.

Nandini, K., Yaramsetty, A., & Tulasirama, M. (2024). Enhancing Cybersecurity Resilience: A Study of Threat Detection and Mitigation Techniques in Modern Networks. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).

Presekal, A., Štefanov, A., Rajkumar, V. S., & Palensky, P. (2023). Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Transactions on Smart Grid.* https://doi.org/10.1109/TSG.2023.10017381

Reda, H. T., Anwar, A., Mahmood, A. N., & Tari, Z. (2023). A taxonomy of cyber defence strategies against false data attacks in smart grids. *ACM Computing Surveys*, *55*(14s), 1-37.

Rithani, M., Kumar, R. P., & Doss, S. (2023). A review on big data based on deep neural network approaches. *Artificial Intelligence Review*, *56*(12), 14765-14801.

Ruben, C., Dhulipala, S., Nagaraj, K., Zou, S., Starke, A., Bretas, A., Zare, A., & McNair, J. (2020). Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. *IET Smart Grid*, 3(4), 445–453. https://doi.org/10.1049/iet-stg.2019.0272

Sagu, A., Gill, N. S., Gulia, P., Priyadarshini, I., & Chatterjee, J. M. (2025). Hybrid optimization algorithm for detection of security attacks in IoT-enabled cyber-physical systems. *IEEE Transactions on Big Data,* 11(1), 35–46. https://doi.org/10.1109/TBDATA.2024.3372368

Sahani, N., Zhu, R., Cho, J. H., & Liu, C. C. (2023). Machine learning-based intrusion detection for smart grid computing: A survey. *ACM Transactions on Cyber-Physical Systems*, *7*(2), 1-31.

Sakhnini, J., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2021). Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. *Physical Communication*, 47, 101394. https://doi.org/10.1016/j.phycom.2021.101394

Sharma, A., Rani, S., Shah, S. H., Sharma, R., Yu, F., & Hassan, M. M. (2023). An efficient hybrid deep learning model for denial of service detection in cyber physical systems**.** *IEEE Transactions on Network Science and Engineering,* 10(5), 2419–2428. https://doi.org/10.1109/TNSE.2023.10123694

Zheng, T., Liu, M., Puthal, D., Yi, P., Wu, Y., & He, X. (2022). Smart grid: Cyber attacks, critical defense approaches, and digital twin. *arXiv preprint arXiv:2205.11783*.

Zibaeirad, A., Koleini, F., Bi, S., Hou, T., & Wang, T. (2024). A comprehensive survey on the security of smart grid: Challenges, mitigations, and future research opportunities.