International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Mitigating Cyber Risks in Smart Cyber-Physical Power Systems Through Deep Learning and Hybrid Security Models

Gurram Sravani
PG, Department of Computer science engineering, Sree Dattha institute of engineering and science, Hyderabad, Telangana, india-501510.
Email: sravaninetha6@gmail.com

k. Madhavi
Associates professor, Department of Computer science engineering, Sree Dattha institute of engineering and science, Hyderabad, Telangana, India -501510.
E-mail: madhavi.k@sreedattha.ac.in

Abstract: The increasing integration of smart cyber physical power systems with communication networks has increased exposure to cyber threats, requiring advanced intrusion detection solutions. This work presents a deep learning based framework using the Cybersecurity Intrusion Simulated Network dataset and PSCAD generated cyber threat scenarios. Data preprocessing includes standardization, categorical encoding, and SMOTEENN sampling. Multiple models, namely Convolutional Neural Network, Long Short Term Memory, Transformer, and a hybrid CNN LSTM architecture, are trained with hyperparameter optimization. Experimental evaluation shows that the CNN LSTM hybrid achieves the highest performance, reaching 95.3% accuracy and 94.4% F1 score on the Cyber Threat dataset, and 99.9% accuracy with 99.9% F1 score on PSCAD simulations. Explainable AI techniques, including LIME and SHAP, are integrated to interpret feature contributions and enhance trust. For practical deployment, the optimized model is implemented using a Flask based web application enabling real time monitoring. The system classifies grid traffic into no attack, attack detected, injection attack, MITM, replay attack, and spoofing attack categories. The proposed approach delivers accurate, interpretable, and scalable intrusion detection for resilient smart grid cybersecurity operations worldwide deployments.

"Index Terms: *Smart cyber-physical power systems (CPPS), cybersecurity in smart grids, renewable energy integration, machine learning for cyber threat detection, deep learning models (CNN, LSTM)".*

1. INTRODUCTION

The rapid transition toward renewable energy integration has significantly transformed the structure and operation of modern power systems, leading to the development of Smart Grids and Cyber-Physical Power Systems (CPPS) [1]. These systems integrate physical power infrastructure with advanced communication and information technologies, enabling real-time monitoring, control, and coordination of power generation, transmission, and distribution [2]. By incorporating distributed energy resources such as solar and wind energy, CPPS enhances the sustainability, efficiency, and flexibility of power networks, aligning with global sustainable development goals [3]. However, the decentralization of energy sources introduces operational complexities, including

challenges in supply-demand balancing, power quality maintenance, and equipment stability [4].

The convergence of cyber and physical layers in CPPS creates new security vulnerabilities, as the communication infrastructure connecting these domains becomes a potential target for cyber-attacks [5]. Threats such as false data injection (FDI), denial-of-service (DoS), and replay attacks can compromise system integrity, disrupt operations, and lead to significant economic and societal consequences [6]. Such vulnerabilities highlight the need for intelligent and adaptive security mechanisms capable of responding to evolving cyber threats. Traditional protection methods often fail to address the dynamic and heterogeneous nature of modern power systems, emphasizing the importance of data-driven approaches [7].

Recent research suggests that integrating advanced machine learning and reinforcement learning techniques into intrusion detection systems can improve CPPS security by enabling real-time detection and mitigation of attacks [8]. Additionally, multi-source and multi-domain data fusion methods allow for the identification of complex attack patterns spanning multiple layers of the power system, increasing detection accuracy and resilience [9]. Feature extraction, co-training, and hybrid learning strategies further contribute to robust cybersecurity solutions capable of adapting to changing threats [10].

2. LITERATURE REVIEW

The increasing integration of renewable energy into power systems and the development of smart grids have introduced significant advancements, along with substantial cybersecurity challenges. Ding et al. [11] provide a comprehensive review of cyber threats to smart grids, offering a taxonomy of attacks, potential mitigation strategies, and future research directions. They highlight how modern smart grids, while improving operational efficiency, create vulnerabilities in communication networks and data management layers that can be exploited by cyber adversaries. Bouramdane [12] explores the challenges of cyber-attacks in smart grids and emphasizes the importance of multi-criteria decision-making for cybersecurity options, including artificial intelligence-based solutions, using an analytical hierarchy process. This method enables systematic evaluation of multiple defense strategies while considering operational and economic constraints.

Wang et al. [13] focus on applying machine learning to detect power grid disturbances and cyber-attacks, demonstrating the ability of data-driven techniques to recognize anomalous patterns and distinguish between faults caused by physical disturbances and malicious cyber activities. Mirzaee et al. [14] extend this discussion by analyzing conventional and machine learning-based approaches for smart grid security, addressing threats and countermeasures in detail. Their study shows how advanced learning models can overcome the limitations of traditional signature-based intrusion detection systems, particularly in detecting previously unseen attack scenarios. Karimipour et al. [15] introduce a deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. Their system can handle massive streaming data while identifying irregularities without requiring labeled attack datasets, making it suitable for complex, real-world grid environments.

Ismail et al. [16] investigate deep learning methods to detect electricity theft and cyber-attacks in renewable distributed generation systems. Their approach addresses the dual challenge of protecting both physical energy assets and cyber information while ensuring distributed energy reliability.

Muhammad et al. [17] provide a survey of cybersecurity protocols and datasets in smart grids, emphasizing the need for comprehensive datasets and standardized evaluation benchmarks for designing effective intrusion detection systems and validating machine learning models. Similarly, Gómez et al. [18] focus on generating anomaly detection datasets in industrial control systems, contributing to realistic test environments for evaluating cyber-defense mechanisms in complex cyber-physical infrastructures.

Bartolini et al. [19] explore the integration of energy storage and multi-energy systems within local energy communities under high renewable penetration. Their research highlights operational challenges introduced by intermittent energy sources and demonstrates the critical role of storage systems in maintaining grid stability. Alam et al. [20] analyze the challenges and solutions associated with high levels of renewable energy penetration in grid utilities, discussing technical issues in voltage regulation, frequency stability, and protection system coordination while emphasizing intelligent control strategies and adaptive monitoring systems to ensure resilient operations. Collectively, these studies illustrate the increasing complexity of modern smart grids, where the interaction between renewable integration, operational efficiency, and cybersecurity creates a multifaceted research landscape.

3. MATERIALS AND METHODS

The proposed system enhances cybersecurity in smart cyber-physical power systems by leveraging advanced deep learning architectures to detect and mitigate [21] cyber threats. It integrates CNN, LSTM, and Transformer models to capture spatial and temporal patterns in network traffic and intrusion datasets, with [23] CNNs extracting hierarchical features, LSTMs modeling sequential dependencies, and Transformers handling long-range contextual relationships in large-scale time-series data. PSCAD simulations generate realistic cyber-attack scenarios to ensure model generalization to practical power system environments. A hybrid [24] CNN+LSTM model further improves detection accuracy, while Explainable AI techniques, LIME and SHAP, provide transparent insights into feature importance. A Flask-based web interface enables data input, prediction visualization, and interpretability, creating a scalable, adaptive, and user-friendly framework for real-time cyber threat detection.

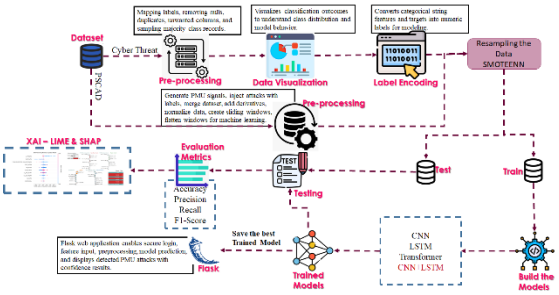


Fig.1 Proposed Architecture

Fig. 1 illustrates a machine learning pipeline for cyber threat detection in power systems. The process begins with dataset ingestion from PSCAD, followed by preprocessing, visualization, and label encoding. After SMOTEENN resampling, the data is split for model building using architectures like CNN+LSTM. Finally, the system undergoes evaluation via XAI techniques and metrics, with the best model deployed through a Flask web application.

a) Dataset Collection:

i) Cyber Threat Dataset Collection: The NF-ToN-IoT dataset was collected from a large-scale IoT network traffic environment, consisting of 1,157,994 records and 12 attributes. It includes

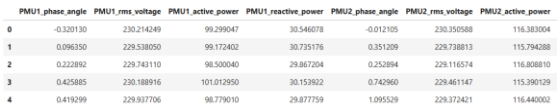
various network features such as source and destination addresses, protocol types, and flow metrics. [22] The dataset contains multiple cyberattack types including Injection, Spoofing, Replay, and MITM, along with normal traffic samples.



	L4_SRC_PORT	L4_DST_PORT	PROTOCOL	L7_PROTO	IN_BYTES	OUT_BYTES	IN_PKTS	OUT_PKTS	TCP_FLAGS	FLOW_DURATION_MILLISECONDS	Label	Attack	Target
0	60641	53	17	5.0	108	108	2	2	0	4	1	dos	Spoofing Attack
1	60641	53	17	5.0	108	108	2	2	0	4	1	injection	Injection Attack
2	60641	53	17	5.0	108	108	2	2	0	4	1	ddos	Spoofing Attack
3	38524	53	17	5.0	100	100	2	2	0	5	1	injection	Injection Attack
4	38524	53	17	5.0	100	100	2	2	0	5	1	ddos	Spoofing Attack

Fig.2 Cyber Threat Dataset

ii) PSCAD Dataset Collection: The PSCAD/PMU dataset was generated synthetically using simulated power system signals from seven Phasor Measurement Units (PMUs), [25] each recording four key parameters—voltage magnitude, angle, frequency, and phase. It includes a total of 60,000 samples representing both normal operations and cyberattack scenarios such as False Data Injection (FDIA), MITM, Replay, and GPS Spoofing attacks.



	PMU1_phase_angle	PMU1_rms_voltage	PMU1_active_power	PMU1_reactive_power	PMU2_phase_angle	PMU2_rms_voltage	PMU2_active_power
0	-0.320130	230.214249	99.299047	30.546078	-0.012105	230.350588	116.383004
1	0.096350	229.538050	99.172402	30.735176	0.351209	229.738813	115.794288
2	0.222892	229.743110	98.500040	29.867204	0.252894	229.116574	116.808810
3	0.425885	230.188916	101.012950	30.153922	0.742960	229.461147	115.390129
4	0.419299	229.937706	98.779010	29.877759	1.095529	229.372421	116.440002

Fig.3 PSCAD Dataset

b) Pre-Processing:

The preprocessing phase ensures data quality and readiness for model training through systematic steps, including cleaning, feature engineering, visualization, sampling, and dataset splitting to enhance accuracy and performance.

i) Data Processing: In this stage, irrelevant columns and unnecessary labels such as *Benign* and *Ransomware* were removed to refine the dataset. Categorical labels representing different attack types were converted into numerical format using LabelEncoder to enable model compatibility. Subsequently, all numerical features were standardized using StandardScaler, ensuring uniform data scaling and improving model convergence by minimizing feature dominance and maintaining consistent input distributions across all features.

ii) Feature Engineering: Relevant features were carefully selected while excluding timestamps and identifiers to reduce redundancy. For the PSCAD dataset, derivative-based features were generated to represent the rate of change in system parameters, enhancing detection accuracy. Additionally, a sliding window approach with a window size of 30 and stride of 5 was applied to transform continuous time-series data into sequential input samples suitable for temporal deep learning models.

iii) Data Visualization: To better understand dataset characteristics, matplotlib and seaborn libraries were used for data visualization. Class distributions were plotted to identify imbalances and evaluate the effects of resampling. Visual representations provided insights into the variation between normal and attack samples, aiding in the verification of preprocessing steps and ensuring the datasets were well-prepared for subsequent model training and performance analysis.

iv) Sampling and Balancing: The SMOTEENN (Synthetic Minority Oversampling Technique combined with Edited Nearest Neighbors) approach was used to address class imbalance in both datasets. [26] SMOTE generated synthetic samples for underrepresented attack classes, while ENN removed overlapping or noisy samples. This hybrid resampling ensured balanced and cleaner data distributions, enhancing model generalization and improving the reliability of classification performance across all attack categories.

c) Training and Testing:

The preprocessed and balanced data were divided into 80% training and 20% testing sets using the train_test_split function. This separation ensured that models were trained on sufficient data while preserving unseen samples for evaluation. The resulting training and testing sets were then formatted into appropriate tensor structures compatible with CNN and other hybrid deep learning architectures for efficient model training and validation.

d) Algorithms:

CNN: Convolutional Neural Networks automatically extract hierarchical spatial features from network traffic and PSCAD simulations, detecting anomalies and malicious activities. [27] They capture local dependencies, reduce dimensionality, and identify attack signatures or system disturbances, enhancing detection accuracy and model generalization.

$$S(i,j) = \sum_{m}\sum_{n} I(i+m, j+n) \cdot K(m,n) \quad (1)$$

LSTM: Long Short-Term Memory networks model long-term temporal dependencies in sequential [28] Cyber Threat data and PSCAD simulations. They capture evolving attack patterns and cascading disturbances, retaining relevant information across time steps while mitigating vanishing gradients, improving recognition of temporal anomalies and complex sequences.

$$h_t = \sigma(w_o \cdot [h_{t-1}, x_t] + b_o) \cdot \tanh(C_t) \quad (2)$$

Transformer: Transformers leverage attention mechanisms to capture long-range dependencies and contextual relationships in network flows and PSCAD simulations. [29] They identify critical patterns across features, handle large-scale data efficiently, and complement spatial and temporal models, enhancing detection of complex attacks and disturbances.

CNN+LSTM: The hybrid CNN+LSTM model combines spatial feature extraction and temporal memory to detect anomalies in network traffic and simulated disturbances. [30] It simultaneously learns local patterns and sequential dependencies, improving accuracy, F1-score, and robustness for recognizing complex cyber-physical system attack scenarios.

e) Integration of XAI and Flask Framework

The integration of Explainable Artificial Intelligence (XAI) with the Flask framework enables transparent and interpretable machine learning model predictions for both Cyber Threat and PSCAD datasets. XAI techniques, such as SHAP or LIME, provide visual explanations of model decisions by highlighting feature contributions and attack patterns. This transparency helps understand why a model flags a network flow or system disturbance as malicious, fostering trust and facilitating debugging.

Flask, a lightweight Python web framework, serves as the deployment layer for these interpretable models. It allows the creation of interactive web interfaces where users can input network or PMU data and receive real-time predictions along with explainable visualizations. The combined XAI-Flask system supports user-friendly monitoring, rapid anomaly detection, and effective decision-making in smart cyber-physical power systems.

4. EXPERIMENTAL RESULTS

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true

negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} (3)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (4)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN} (5)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

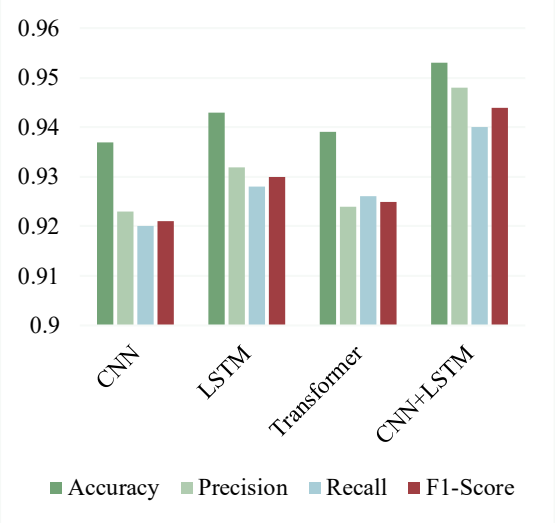
$$F1\ Score = 2 * \frac{Recall\ X\ Precision}{Recall + Precision} * 100 (6)$$

Table.1 Performance Evaluation Table– Cyber Threat Data

ML Model	Accuracy	Precision	Recall	F1-Score
CNN	0.937	0.923	0.920	0.921
LSTM	0.943	0.932	0.928	0.930
Transformer	0.939	0.924	0.926	0.925
CNN+LSTM	**0.953**	**0.948**	**0.940**	**0.944**

In Table.1, CNN+LSTM achieves the highest performance, demonstrating superior accuracy and reliability compared to the other evaluated models.

Fig.4 Comparison Graph– Cyber Threat Data



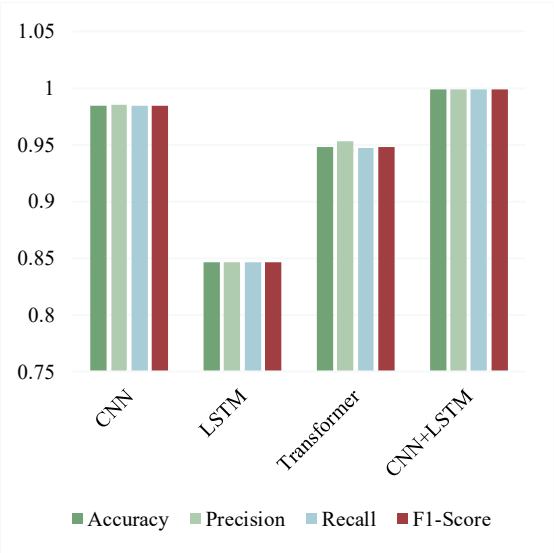
In fig.4, CNN+LSTM shows the highest performance. Accuracy is represented in green, precision in light green, recall in blue, and F1-score in red, highlighting its superior results.

Table.2 Performance Evaluation – PSCAD

ML Model	Accuracy	Precision	Recall	F1-Score
CNN	0.984	0.985	0.984	0.984
LSTM	0.846	0.846	0.846	0.846
Transformer	0.948	0.953	0.947	0.948
CNN+LSTM	**0.999**	**0.999**	**0.999**	**0.999**

In Table.2, CNN+LSTM achieves the highest performance, demonstrating exceptional detection capability compared to the other evaluated models.

Fig.5 Comparison Graph – PSCAD



In fig.5, CNN+LSTM achieves the highest performance. Accuracy is represented in green, precision in light green, recall in blue, and F1-score in red, highlighting its superior detection capability.

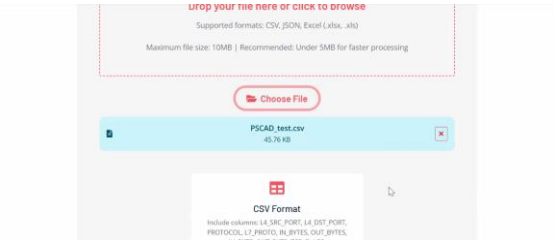


Fig.6 Upload Input File

Fig.6 illustrates an input interface where users can drag-and-drop or browse files to upload and obtain automated analysis results efficiently.

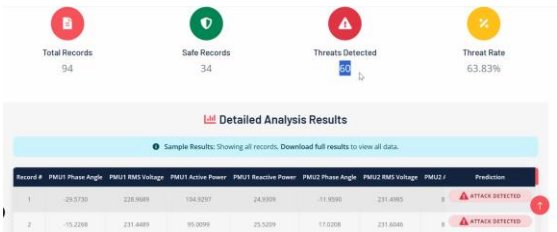


Fig.7 Predicted Results

Fig.7 presents the output interface displaying detailed analysis of 94 records with predictions as "Attack Detected" or "Normal," indicating 34 safe, 60 threats detected, and a threat rate of 63.83%.

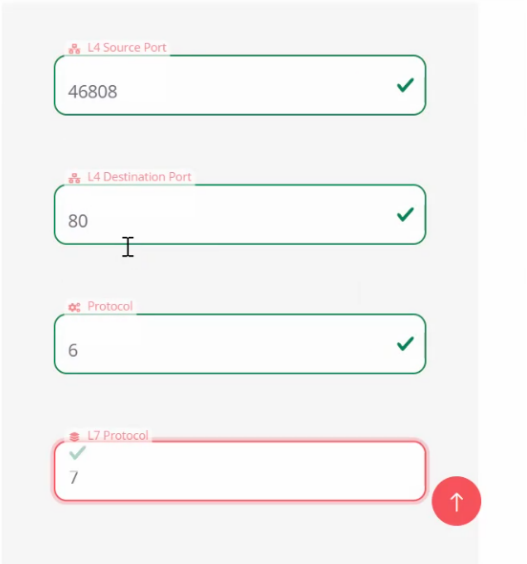


Fig.8 Enter Input Data

Fig.8 illustrates an input interface allowing users to enter Cyber Threat data, enabling automated prediction of results efficiently and accurately.

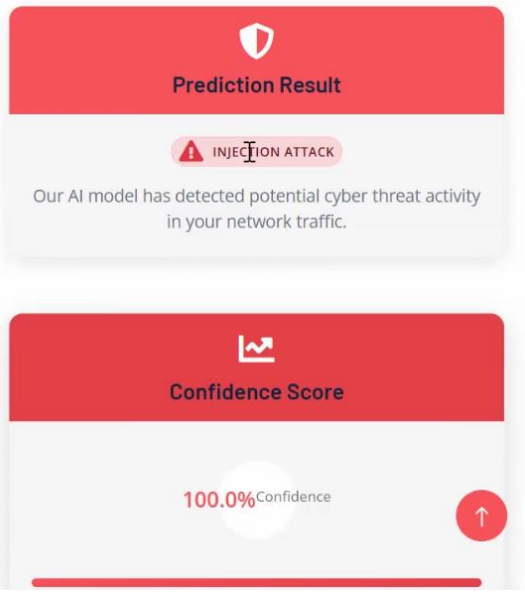


Fig.9 Predicted Results

Fig.9 presents the output interface displaying the prediction result as "Injection Attack" with a

confidence score of 100%, indicating accurate detection.

5. CONCLUSION

The integration of deep learning and hybrid security frameworks has demonstrated strong potential in mitigating cyber risks within cyber-physical power systems. By employing the Cybersecurity Intrusion Simulated Network dataset alongside PSCAD-based simulations, a robust evaluation was achieved across multiple learning settings. Preprocessing strategies, including feature standardization and SMOTEENN sampling, improved data quality and learning efficiency. The hybrid CNN+LSTM model emerged as the highest-performing approach, achieving 95.3% accuracy and 94.4% F1-score on the Cyber Threat dataset, and 99.9% accuracy with a 99.9% F1-score on PSCAD simulations. These results confirm its ability to capture spatial and temporal intrusion characteristics more effectively than conventional standalone models. Explainable artificial intelligence techniques, namely LIME and SHAP, enhanced transparency by identifying influential features, supporting trust and informed decision-making in critical infrastructures. For operational deployment, the optimized model is implemented using a Flask-based web framework that enables real-time monitoring and interaction. The system classifies events into no attack, attack detected, injection attack, MITM, replay attack, and spoofing attack, allowing timely mitigation actions. Overall, the framework provides a scalable, interpretable, and high-accuracy cybersecurity solution for resilient grid protection.

Future work will focus on expanding the scope of cyber risk mitigation in smart cyber-physical power systems by incorporating real-time streaming data to enhance detection capabilities under dynamic conditions. Large-scale deployment scenarios will be explored using diverse datasets that integrate both IT and operational technology (OT) environments, ensuring broader generalizability. Advanced ensemble learning and federated learning approaches may be adopted to improve resilience while preserving data privacy across distributed infrastructures. Furthermore, optimization techniques will be applied to reduce computational overhead, enabling lightweight models suitable for edge devices in power grids. Attention will also be directed towards developing adaptive intrusion response mechanisms that not only detect but also mitigate threats proactively to strengthen overall grid security.

REFERENCES

[1] Ruan, J., Liang, G., Zhao, J., Zhao, H., Qiu, J., Wen, F., & Dong, Z. Y. (2023). Deep learning for cybersecurity in smart grids: Review and perspectives. Energy Conversion and Economics, 4(4), 233-251.

[2] Hasan, M. K., Abdulkadir, R. A., Islam, S., Gadekallu, T. R., & Safie, N. (2024). A review on machine learning techniques for secured cyber-physical systems in smart grid networks. Energy Reports, 11, 1268-1290.

[3] Alam, K., Al Imran, M., Mahmud, U., & Al Fathah, A. (2024). Cyber attacks detection and mitigation using machine learning in smart grid systems. Journal of Science and Engineering Research, November, 12.

[4] Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., & Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. Applied Energy, 383, 125364.

[5] Mejia-Ruiz, G. E., Marasini, G., Zhihua, Q., Kundu, S., & Pushpak, S. (2025). Cybersecurity

challenges in power networks with distributed energy resources: A comprehensive survey. Renewable and Sustainable Energy Reviews, 224, 116100.

[6] M. A. S. P. Dayarathne, M. S. M. Jayathilaka, R. M. V. A. Bandara, V. Logeeshan, S. Kumarawadu, and C. Wanigasekara, ‘‘Deep learning-based cyber attack detection in power grids with increasing renewable energy penetration,’’ in Proc. IEEE World AI IoT Congr. (AIIoT), Seattle, WA, USA, May 2024, pp. 521–526, doi: 10.1109/AIIoT61789.2024.10578979.

[7] I. Alotaibi, M. A. Abido, M. Khalid, and A. V. Savkin, ‘‘A comprehensive review of recent advances in smart grids: A sustainable future with renew able energy resources,’’ Energies, vol. 13, no. 23, p. 6269, Nov. 2020, doi: 10.3390/en13236269.

[8] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, ‘‘Cyber-physical power system (CPPS): A review on modeling, simula tion, and analysis with cyber security applications,’’ IEEE Access, vol. 8, pp. 151019–151064, 2020, doi: 10.1109/ACCESS.2020.3016826.

[9] Erdiwansyah, Mahidin, H. Husin, Nasaruddin, M. Zaki, and Muhibbuddin, ‘‘A critical review of the integration of renewable energy sources with various technologies,’’ Protection Control Mod. Power Syst., vol. 6, no. 1, Dec. 2021, Art. no. 3, doi: 10.1186/s41601-021-00181-3.

[10] F. Ahsan, N. H. Dana, S. K. Sarker, L. Li, S. M. Muyeen, M. F. Ali, Z. Tasneem, M. M. Hasan, S. H. Abhi, M. R. Islam, M. H. Ahamed, M. M. Islam, S. K. Das, M. F. R. Badal, and P. Das, ‘‘Data-driven next generation smart grid towards sustainable energy evolution: Techniques andtechnologyreview,’’ Protection Control Mod. PowerSyst., vol. 8, no. 1, pp. 1–42, Dec. 2023, doi: 10.1186/s41601-023-00319-5.

[11] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, ‘‘Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions,’’ Energies, vol. 15, no. 18, p. 6799, Sep. 2022, doi: 10.3390/en15186799.

[12] A.-A. Bouramdane, ‘‘Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process,’’ J. Cybersecur. Privacy, vol. 3, no. 4, pp. 662–705, Sep. 2023, doi: 10.3390/jcp3040031.

[13] D. Wang, X. Wang, Y. Zhang, and L. Jin, ‘‘Detection of power grid disturbances and cyber-attacks based on machine learning,’’ J. Inf. Secur. Appl., vol. 46, pp. 42–52, Jun. 2019, doi: 10.1016/j.jisa.2019.02.008.

[14] P. H. Mirzaee, M. Shojafar, H. Cruickshank, and R. Tafazolli, ‘‘Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures),’’ IEEE Access, vol. 10, pp. 52922–52954, 2022, doi: 10.1109/ACCESS.2022.3174259.

[15] H. Karimipour, A. Dehghantanha, R. M. Parizi, K. R. Choo, and H. Leung, ‘‘A deep and scalable unsupervised machine learning sys tem for cyber-attack detection in large-scale smart grids,’’ IEEE Access, vol. 7, pp. 80778–80788, 2019, doi: 10.1109/ACCESS.2019. 2920326.

[16] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, ‘‘Deep learning detection of electricity theft cyber-attacks in renewable distributed gener ation,’’ IEEE Trans. Smart Grid, vol. 11, no. 4, pp.

3428–3437, Jul. 2020, doi: 10.1109/TSG.2020.2973681.

[17] M. Muhammad, A. S. Alshra'a, and R. German, ''Survey of cybersecurity in smart grids protocols and datasets,'' Proc. Comput. Sci., vol. 241, pp. 365–372, Mar. 2024, doi: 10.1016/j.procs.2024.08.049.

[18] Á. L. P. Gómez, L. F. Maimó, A. H. Celdrán, F.J.G. Clemente, C. C. Sarmiento, C. J. D. C. Masa, and R. M. Nistal, ''On the genera tion of anomaly detection datasets in industrial control systems,'' IEEE Access, vol. 7, pp. 177460–177473, 2019, doi: 10.1109/ACCESS.2019. 2958284.

[19] A. Bartolini, F. Carducci, C. B. Muñoz, and G. Comodi, ''Energy storage and multi energy systems in local energy communities with high renewable energy penetration,'' Renew. Energy, vol. 159,pp. 595–609,Oct.2020,doi: 10.1016/j.renene.2020.05.131.

[20] Md. S. Alam, F. S. Al-Ismail, A. Salem, and M. A. Abido, ''High level penetration of renewable energy sources into grid utility: Challenges and solutions,'' IEEE Access, vol. 8, pp. 190277–190299, 2020, doi: 10.1109/ACCESS.2020.3031481.

[21] R. Qi, C. Rasband, J. Zheng, and R. Longoria, ''Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning,'' Information, vol. 12, no. 8, p. 328, Aug. 2021, doi: 10.3390/info12080328.

[22] K. Zarzycki, P. Chaber, K. Cabaj, M. Ławryńczuk, P. Marusak, R. Nebeluk, S. Plamowski, and A. Wojtulewicz, ''Forgery cyber-attack supported by LSTM neural network: An experimental case study,'' Sensors, vol. 23, no. 15, p. 6778, Jul. 2023, doi: 10.3390/s23156778.

[23] M. Farajzadeh-Zanjani, E. Hallaji, R. Razavi-Far, M. Saif, and M. Parvania, ''Adversarial semi-supervised learning for diagnosing faults and attacks in power grids,'' IEEE Trans. Smart Grid, vol. 12, no. 4, pp. 3468–3478, Jul. 2021, doi: 10.1109/TSG.2021.3061395.

[24] A. Almalaq, S. Albadran, and M. Mohamed, ''Deep machine learning model-based cyber-attacks detection in smart power systems,'' Mathemat ics, vol. 10, no. 15, p. 2574, Jul. 2022, doi: 10.3390/math10152574.

[25] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, ''An ensemble deep learning-based cyber-attack detection in industrial control system,'' IEEE Access, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[26] F. Khan, R. Alturki, M. A. Rahman, S. Mastorakis, I. Razzak, and S. T. Shah, ''Trustworthy and reliable deep-learning-based cyberattack detection in industrial IoT,'' IEEE Trans. Ind. Informat., vol. 19, no. 1, pp. 1030–1038, Jan. 2023, doi: 10.1109/TII.2022.3190352.

[27] W. Wang, F. Harrou, B. Bouyeddou, S.-M. Senouci, and Y. Sun, ''Cyber attacks detection in industrial systems using artificial intelligence-driven methods,'' Int. J. Crit. Infrastruct. Protection, vol. 38, Sep. 2022, Art. no. 100542, doi: 10.1016/j.ijcip.2022.100542.

[28] K. Swathi and G. Narsimha, ''Robust deep learning based framework for detecting cyber attacks from abnormal network traffic,'' Int. J. Recent Innov. Trends Comput. Commun., vol. 11, no. 7, pp. 341–353, Sep. 2023, doi: 10.17762/ijritcc.v11i7.7958.

[29] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, ‘‘Cybersecurity in power grids: Challenges and opportunities,’’ Sensors, vol. 21, no. 18, p. 6225, Sep. 2021, doi: 10.3390/s21186225.

[30] Dayarathne, M. A. S. P., Jayathilaka, M. S. M., Bandara, R. M. V. A., Logeeshan, V., Kumarawadu, S., & Wanigasekara, C. (2024, May). Deep learning-based cyber attack detection in power grids with increasing renewable energy penetration. In 2024 IEEE World AI IoT Congress (AIIoT) (pp. 521-526). IEEE.