Intelligent Deep Learning Approach for Detecting Cyber Attacks in Smart Power Grid Communication Systems

G Viswanath [1], M Vedavathi [2]

[1]Associate Professor, Department of CSE(AI & ML), Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: viswag111@gmail.com, ORC-ID: https://orcid.org/0009-0001-7822-4739

[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: melamvarsha5@gmail.com , ORC-ID: https://orcid.org/0009-0001-8554-1900

Abstract: The growing integration of intelligent cyber-physical power systems with communication networks has heightened vulnerability to cyber attacks, necessitating sophisticated intrusion detection technologies. This study introduces a deep learning architecture utilizing the Cybersecurity Intrusion Simulated Network dataset and PSCAD-generated cyber threat scenarios. Data preprocessing encompasses normalization, category encoding, and SMOTEENN sampling. Various models, specifically Convolutional Neural Network, Long Short Term Memory, Transformer, and a hybrid CNN LSTM architecture, are trained utilizing hyperparameter optimization. Experimental assessment indicates that the CNN LSTM hybrid attains superior performance, with 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. Explainable AI methodologies, such as LIME and SHAP, are employed to elucidate feature contributions and bolster trust. The optimized model is deployed using a Flask-based web application, facilitating real-time monitoring. The system categorizes grid traffic into the following classifications: no attack, assault identified, injection attack, man-in-the-middle (MITM) attack, replay attack, and spoofing attack. The suggested method provides precise, comprehensible, and scalable intrusion detection for robust smart grid cybersecurity operations in global implementations.

"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 swift shift to renewable energy integration has profoundly altered the architecture and functioning of contemporary power systems, resulting in the emergence of Smart Grids and Cyber-Physical Power Systems (CPPS) [1]. These systems amalgamate physical power infrastructure with sophisticated communication and information technologies, facilitating real-time monitoring, control, and coordination of power generation, transmission, and distribution [2]. CPPS promotes the sustainability, efficiency, and flexibility of power networks by integrating dispersed energy resources, including solar and wind energy, in accordance with global sustainable development objectives [3]. The decentralization of energy sources presents operational issues, such as difficulties in balancing supply and demand, maintaining power quality, and ensuring equipment stability [4].

The integration of cyber and physical layers in Cyber-Physical Production Systems (CPPS) generates novel security risks, since the communication infrastructure linking these domains

becomes a prospective target for cyber-attacks [5]. Threats including false data insertion (FDI), denial-of-service (DoS), and replay assaults can undermine system integrity, disrupt operations, and result in substantial economic and societal repercussions [6]. These weaknesses underscore the necessity for sophisticated and adaptable security measures that can address the changing landscape of cyber threats. Conventional protection methods frequently neglect the dynamic and diverse characteristics of contemporary power systems, highlighting the necessity of data-driven strategies [7].

Recent studies indicate that incorporating sophisticated machine learning and reinforcement learning methodologies into intrusion detection systems can enhance the security of Cyber-Physical Production Systems (CPPS) by facilitating real-time identification and alleviation of intrusions [8]. Furthermore, multi-source and multi-domain data fusion techniques facilitate the recognition of intricate assault patterns across several layers of the power system, hence enhancing detection precision and robustness [9]. Feature extraction, co-training, and hybrid learning methodologies enhance resilient cybersecurity solutions that can adapt to evolving threats [10].

2. LITERATURE REVIEW

The growing incorporation of renewable energy into power systems and the evolution of smart grids have brought notable progress, accompanied by considerable cybersecurity difficulties. Ding et al. [11] present an exhaustive analysis of cyber threats to smart grids, including a classification of attacks, possible mitigation techniques, and prospective research avenues. They emphasize that contemporary smart grids, albeit enhancing operational efficiency, introduce weaknesses in communication networks and data management systems that might be exploited by cyber adversaries. Bouramdane [12] examines the issues posed by cyber-attacks in smart grids and underscores the significance of multi-criteria decision-making for cybersecurity strategies, incorporating artificial intelligence-based solutions through an analytical hierarchy approach. This approach facilitates the systematic assessment of various defense tactics, taking into account operational and fiscal limitations.

Wang et al. [13] concentrate on utilizing machine learning to identify power grid disturbances and cyber-attacks, illustrating the capacity of data-driven methodologies to discover aberrant patterns and differentiate between faults resulting from physical disturbances and nefarious cyber actions. Mirzaee et al. [14] expand this discourse by examining traditional and machine learning-based methodologies for smart grid security, thoroughly addressing threats and responses. Their research demonstrates how sophisticated learning models can surpass the constraints of conventional signature-based intrusion detection systems, especially in identifying novel assault scenarios. Karimipour et al. [15] present a profound and scalable unsupervised machine learning framework for the detection of cyber-attacks in extensive smart grids. Their system can process extensive streaming data while detecting anomalies without the need for annotated attack datasets, rendering it appropriate for intricate, real-world grid systems.

Ismail et al. [16] examine deep learning techniques for identifying electricity theft and cyber-attacks in renewable distributed generation systems. Their strategy tackles the dual challenge of safeguarding both physical energy assets and cyber information, while guaranteeing the resilience of distributed energy systems. Muhammad et al. [17] present an overview of cybersecurity protocols and datasets in

smart grids, highlighting the necessity for extensive datasets and consistent evaluation benchmarks to develop effective intrusion detection systems and validate machine learning models. Gómez et al. [18] concentrate on creating anomaly detection datasets for industrial control systems, enhancing realistic testing environments for assessing cyber-defense strategies in intricate cyber-physical infrastructures.

Bartolini et al. [19] investigate the amalgamation of energy storage and multi-energy systems in local energy communities with significant renewable integration. Their research underscores the operational difficulties posed by intermittent energy sources and illustrates the essential function of storage devices in preserving grid stability. Alam et al. [20] examine the challenges and solutions related to significant renewable energy integration in grid utilities, addressing technical concerns in voltage regulation, frequency stability, and protection system coordination, while highlighting intelligent control strategies and adaptive monitoring systems to maintain resilient operations. These works collectively demonstrate the growing intricacy of contemporary smart grids, wherein the interplay of renewable integration, operational efficiency, and cybersecurity forms a complicated study environment.

3. MATERIALS AND METHODS

The suggested method improves cybersecurity in smart cyber-physical power systems by utilizing advanced deep learning architectures to identify and counteract cyber attacks. It incorporates CNN, LSTM, and Transformer models to discern spatial and temporal patterns in network traffic and intrusion datasets, with CNNs extracting hierarchical features, LSTMs modeling sequential dependencies, and Transformers managing long-range contextual relationships in extensive time-series data. PSCAD simulations produce authentic cyber-attack scenarios to guarantee model generalization to real-world power system contexts. A hybrid CNN+LSTM model enhances detection accuracy, while Explainable AI methodologies, LIME and SHAP, offer transparent insights into feature significance. A Flask-based web interface facilitates data entry, prediction visualization, and interpretability, establishing a scalable, adaptive, and user-friendly framework for real-time cyber threat detection.

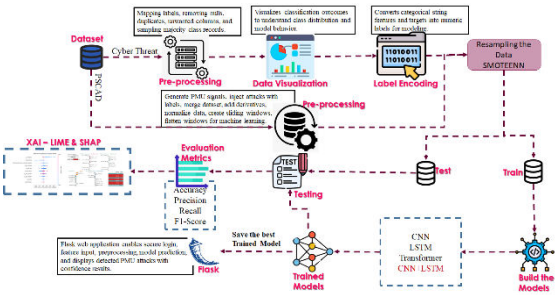


Fig.1 Proposed Architecture

Figure 1 depicts a machine learning pipeline for the detection of cyber threats in power systems. The procedure commences with dataset importation from PSCAD, succeeded by preprocessing, visualization, and label encoding. Subsequent to SMOTEENN resampling, the dataset is partitioned for model development utilizing architectures such as CNN combined with LSTM. The system is ultimately assessed using XAI methodologies and metrics, with the optimal model implemented via a Flask web application.

a) Dataset Collection:

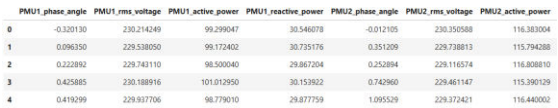
i) Cyber Threat Dataset Collection: The NF-ToN-IoT dataset comprises 1,157,994 records and 12 attributes, sourced from a large-scale IoT network traffic scenario. It encompasses diverse network attributes, including source and destination addresses, protocol types, and flow metrics. The

dataset include many sorts of cyberattacks, including Injection, Spoofing, Replay, and MITM, as well as samples of normal traffic.

	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	ddos	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 synthetically produced with simulated power system signals from seven Phasor Measurement Units (PMUs), each documenting four essential parameters: voltage magnitude, angle, frequency, and phase. The dataset comprises 60,000 samples that encompass both normal operations and cyberattack situations, including False Data Injection (FDIA), Man-in-the-Middle (MITM), Replay, and GPS Spoofing assaults.



	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 preparation phase guarantees data quality and preparedness for model training by systematic procedures, encompassing cleaning, feature engineering, visualization, sampling, and dataset partitioning to improve accuracy and performance.

i) Data Processing: At this point, extraneous columns and superfluous labels, such as Benign and Ransomware, were eliminated to enhance the dataset. Categorical labels denoting various assault kinds were transformed into numerical representation via LabelEncoder to ensure model consistency. All numerical features were subsequently normalized using StandardScaler, providing uniform data scaling, enhancing model convergence by decreasing feature dominance, and keeping consistent input distributions across all features.

ii) Feature Engineering: Relevant features were meticulously chosen, omitting timestamps and identifiers to minimize redundancy. Derivative-based features were created for the PSCAD dataset to capture the rate of change in system parameters, hence improving detection accuracy. A sliding window technique with a window size of 30 and a stride of 5 was employed to convert continuous time-series data into sequential input samples appropriate for temporal deep learning models.

iii) Data Visualization: Matplotlib and seaborn libraries were employed for data visualization to enhance comprehension of dataset properties. Class distributions were graphed to detect imbalances and assess the impact of resampling. Visual representations elucidated the differences between normal and attack samples, facilitating the validation of preprocessing methods and confirming that the datasets were adequately prepared for subsequent model training and performance evaluation.

iv) Sampling and Balancing: The SMOTEENN (Synthetic Minority Oversampling Technique combined with Edited Nearest Neighbors) method was employed to rectify class imbalance in both datasets. SMOTE produced synthetic instances for underrepresented attack categories, whereas ENN eliminated overlapping or noisy instances. This hybrid resampling achieved balanced and refined data distributions, hence strengthening model generalization and augmenting the reliability of classification performance across all attack types.

c) Training and Testing:

The preprocessed and balanced data were partitioned into 80% training and 20% testing sets utilizing the train_test_split tool. This division guaranteed that models were trained on adequate data while retaining unseen samples for assessment. The training and testing data were subsequently organized into suitable tensor structures compatible with CNN and other hybrid deep learning architectures for fast model training and validation.

d) Algorithms:

CNN: Convolutional Neural Networks autonomously extract hierarchical spatial information from network data and PSCAD simulations, identifying anomalies and harmful behaviors. [27] They capture local dependencies, diminish complexity, and discern attack signatures or system anomalies, hence improving detection precision 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 Cyber Threat data and PSCAD simulations. They capture changing assault patterns and cascading disruptions, preserving pertinent information throughout time steps while alleviating fading gradients, hence enhancing the recognition of temporal anomalies and intricate sequences.

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

Transformer: Transformers utilize attention methods to capture long-range dependencies and contextual interactions in network flows and PSCAD simulations. [29] They discern essential patterns among features, manage extensive data proficiently, and augment spatial and temporal models, so improving the identification of intricate attacks and disruptions.

CNN+LSTM: The hybrid CNN+LSTM model integrates spatial feature extraction with temporal memory to identify anomalies in network traffic and simulated disturbances. 30 It concurrently acquires local patterns and sequential dependencies, enhancing accuracy, F1-score, and resilience in identifying intricate cyber-physical system assault scenarios.

e) Integration of XAI and Flask Framework

The amalgamation of Explainable Artificial Intelligence (XAI) with the Flask framework facilitates transparent and interpretable predictions from machine learning models for both Cyber Threat and PSCAD datasets. XAI methodologies, such SHAP and LIME, offer visual elucidations of model decisions by emphasizing feature contributions and identifying attack patterns. This transparency elucidates the rationale behind a model identifying a network flow or system disruption as malicious, hence enhancing trust and aiding in debugging.

Flask, a minimalist Python web framework, functions as the deployment layer for these interpretable models. It facilitates the development of interactive web interfaces that enable users to input network or PMU data and obtain real-time forecasts accompanied by elucidative visuals. The integrated XAI-Flask system facilitates intuitive monitoring, swift anomaly identification, and efficient decision-making in intelligent cyber-physical power systems.

4. EXPERIMENTAL RESULTS

Accuracy: The accuracy of a test refers to its capacity to correctly distinguish between patient and

healthy cases. To assess the accuracy of a test, one must compute the ratio of true positives and true negatives across all assessed cases. This can be expressed mathematically as:

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

Precision: Precision assesses the proportion of accurately classified cases among those identified as positive. Consequently, the formula for calculating precision is expressed as:

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

Recall: Recall is a metric in machine learning that assesses a model's capacity to recognize all pertinent instances of a specific class. It is the proportion of accurately predicted positive observations to the total actual positives, offering insights into a model's efficacy in identifying occurrences of a specific class.

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

F1-Score: The F1 score is a metric for evaluating the accuracy of a machine learning model. It integrates the precision and recall metrics of a model. The accuracy metric quantifies the frequency of true predictions generated by a model throughout the entire dataset.

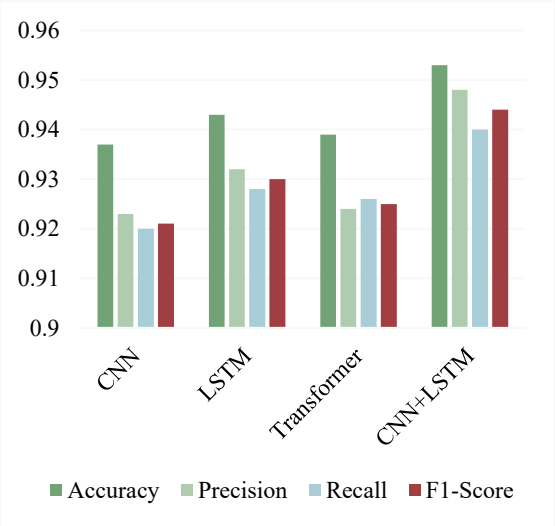
$$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall + Precision} * 100 (6)$$

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 attains the highest performance, exhibiting greater accuracy and dependability than the other assessed models.

Fig.4 Comparison Graph– Cyber Threat Data



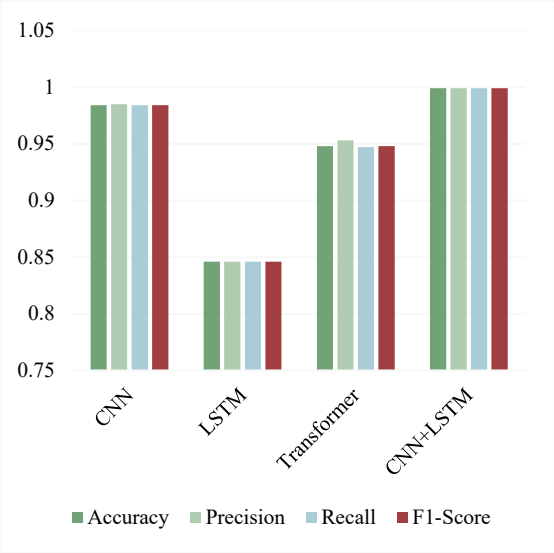
In Figure 4, the CNN+LSTM model demonstrates superior performance. Accuracy is denoted in green, precision in light green, recall in blue, and F1-score in red, emphasizing its exceptional outcomes.

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 attains superior performance, exhibiting remarkable detecting proficiency relative to the other assessed models.

Fig.5 Comparison Graph – PSCAD



In Figure 5, the CNN+LSTM model attains the superior performance. Accuracy is denoted in green, precision in light green, recall in blue, and F1-score in red, emphasizing its enhanced detection proficiency.

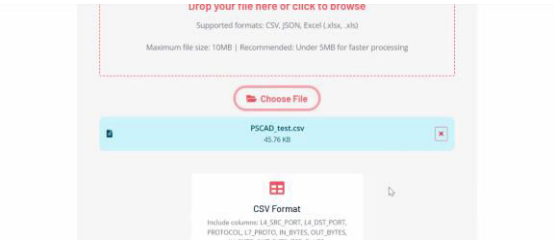


Fig.6 Upload Input File

Figure 6 depicts an input interface that enables users to upload files by drag-and-drop or browsing methods to receive automated analysis results efficiently.

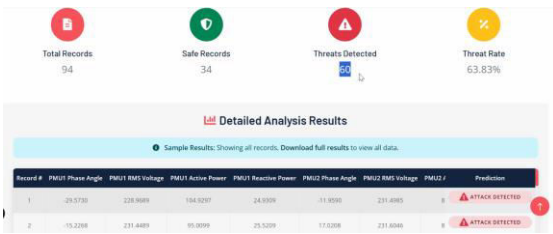


Fig.7 Predicted Results

Figure 7 illustrates the output interface, which provides a comprehensive analysis of 94 records categorized as either “Attack Detected” or “Normal,” revealing 34 instances classified as safe, 60 as threats, and a threat rate of 63.83%.

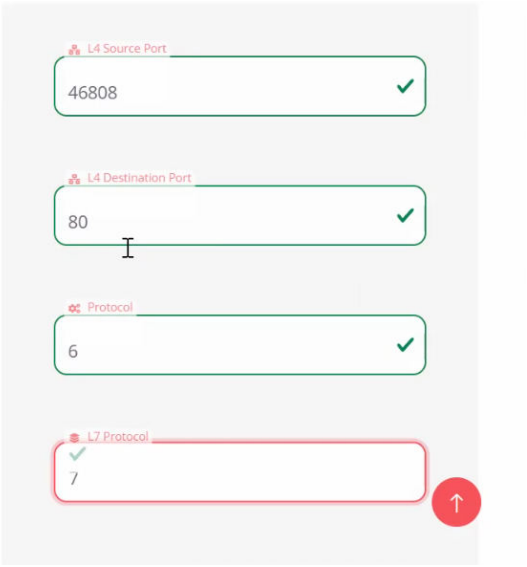


Fig.8 Enter Input Data

Figure 8 depicts an input interface that permits users to input Cyber Threat data, facilitating the efficient and accurate automation of result predictions.

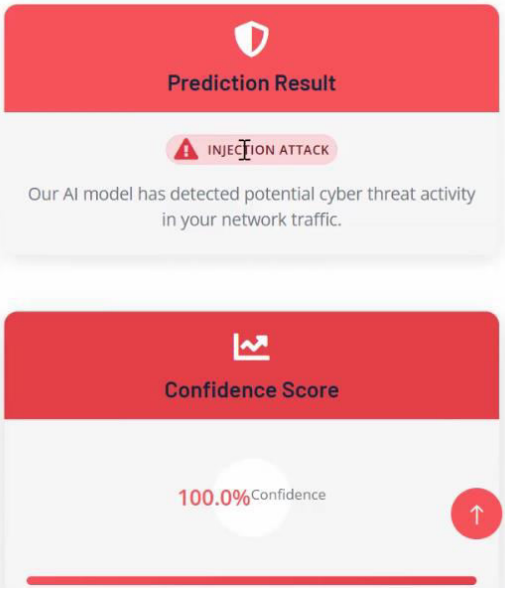


Fig.9 Predicted Results

Figure 9 illustrates the output interface showcasing the prediction outcome as “Injection Attack” with a confidence score of 100%, signifying precise detection.

5. CONCLUSION

The amalgamation of deep learning and hybrid security frameworks has shown significant promise in alleviating cyber hazards in cyber-physical power systems. A comprehensive assessment was conducted utilizing the Cybersecurity Intrusion Simulated Network dataset in conjunction with PSCAD-based simulations across several learning environments. Preprocessing techniques, such as feature standardization and SMOTEENN sampling, enhanced data quality and learning efficacy. The hybrid CNN+LSTM model demonstrated superior performance, attaining 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 validate its capacity to more effectively capture spatial and temporal incursion characteristics compared to traditional standalone models. Explainable artificial intelligence methods, specifically LIME and SHAP, improved transparency by pinpointing significant traits, hence fostering confidence and facilitating informed decision-making in critical infrastructures. The optimized model is deployed operationally using a Flask-based web framework that facilitates real-time monitoring and interactivity. The system categorizes events as no attack, attack identified, injection attack, man-in-the-middle (MITM), replay attack, and spoofing attack, facilitating prompt mitigation measures. The framework offers a scalable, interpretable, and highly accurate cybersecurity solution for robust grid protection.

Future endeavors will concentrate on broadening the parameters of cyber risk mitigation in intelligent cyber-physical power systems by integrating real-time streaming data to improve detection efficacy under fluctuating conditions. Diverse datasets integrating IT and operational technology (OT) systems will be utilized to examine large-scale deployment scenarios, ensuring greater generalizability. Advanced ensemble learning and federated learning methodologies can be employed to enhance resilience while maintaining data privacy in distributed systems. Moreover, optimization methods will be employed to minimize computational overhead, facilitating lightweight models appropriate for edge devices in power grids. Focus will also be placed on creating adaptive intrusion response mechanisms that not only identify but also proactively mitigate threats to enhance 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] Gudditti, V., & Krishna, P. V. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 545–554.

[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] Kumar, K., Udaya Suriya Rajkumar, D., Viswanath, G., & Mahalakshmi, J. (2024). A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System. International Journal of Computing, 23(1), 109–115. https://doi.org/10.47839/ijc.23.1.3442

[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] Dr, K, Pushpa Latha., Mr, M, N, Mallikarjuna Reddy., Dr, B, Rajalingam., Malleswari Akurati., Dr, G, Swapna., Bakkala Santha Kumar. (2026). Blockchain-Enabled Trade Finance Framework for Secure Drug Supply Chain Transactions. International Journal of Drug Delivery Technology, 16(3s), 884–889.

[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] Lakshmi, J. M., Prasad, K. K., & Viswanath, G. (2025). Proactive Security in Multi-Cloud Environments: A Blockchain Integrated Real-Time Anomaly Detection and Mitigation Framework. Cuestiones De Fisioterapia, 54(2), 392–417.