ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Volume 13, Issue 7, July 2026

Cyber Attack Detection in Smart Grid using Machine Learning

[1] Prof. Kiruthika K, [2] B Jnanesh,[3] Vikram J R, [4] Rakshita Hanamant Mathad, [5] Shaik Dilshad

[1] [2] [3] [4] [5] Department of Electrical and Electronics Engineering, Rajrajeswari College of Engineering, Visvesvaraya Technological University, Karnataka, India

Corresponding Author Email: [1] kiruthi.km21@gmail.com, [2] jnaneshb996@gmail.com, [3] vikram2027eeerrce@gmail.com, [4] rakshita2027eeerrce@gmail.com, [5] skdilshadpvp@gmail.com

Abstract*— Smart grids use modern communication, control, and computing technologies to make power systems more efficient, reliable, and sustainable. However, the increased use of connected devices and communication networks also makes smart grids vulnerable to different cyberattacks, including Denial of Service (DoS), data injection, scanning, rogue node, switching, connection loss, and double command attacks. Such attacks can affect grid operation, cause power interruptions, and create financial and safety concerns. This work presents a machine learning-based system for detecting cyberattacks in smart grids using MATLAB and Raspberry Pi 3B+. A publicly available smart grid cybersecurity dataset containing different attack categories is used to train a Bi-lateral Convolutional Neural Network (CNN)-based Artificial Neural Network (ANN) model in MATLAB. The trained model is then deployed on the Raspberry Pi 3B+ for real-time attack detection. A MATLAB App Designer-based GUI is used to provide input data and display the detected attack, while a 16×2 LCD provides a local indication. The proposed system offers a simple, low-cost, portable, and practical approach for real-time cybersecurity monitoring in smart grid environments.

Index Terms*— Artificial Neural Network (ANN), Anomaly Detection, Classification, Cyber Attack Detection, Network Security, Smart Grid Security.

I. INTRODUCTION

Smart grids improve power system efficiency, reliability, and monitoring through advanced technologies but are vulnerable to various cyberattacks. This work proposes a machine learning-based cyberattack detection system using a Bi-lateral CNN-ANN model. MATLAB is used for training and monitoring, while Raspberry Pi 3B+ enables real-time attack detection. The detected attacks are displayed on a GUI and 16×2 LCD for effective cybersecurity monitoring.

II. LITERATURE REVIEW

The increasing integration of communication, sensing, automation, and information technologies has transformed conventional power systems into smart grids. However, the increased connectivity of smart grids also exposes them to various cybersecurity threats, including Denial-of-Service (DoS), false data injection, data manipulation, malware, and unauthorized access. Previous studies have highlighted vulnerabilities in the communication and control layers of cyber-physical power systems and emphasized the need for reliable intrusion detection and security mechanisms [1]–[4].

Machine learning (ML) techniques have been widely investigated for detecting cyberattacks in smart-grid environments. Supervised learning approaches have demonstrated the ability to classify normal and malicious network behaviour using labelled datasets. Feature-selection techniques have also been investigated to identify relevant features and improve classification performance [5], [6]. Computational intelligence and machine-learning-based intrusion detection methods have further demonstrated the potential to improve attack identification and reduce false alarms [7]. Reviews of smart-grid security have highlighted the importance of suitable datasets, feature selection, and adaptive learning techniques for developing effective detection systems [8]–[10].

Researchers have also investigated data-mining, reinforcement-learning, and artificial neural network (ANN) approaches for smart-grid cybersecurity. Data-mining techniques can extract useful patterns from large datasets, while reinforcement learning provides the possibility of adapting detection decisions to changing attack conditions [11]–[13]. Neural-network-based methods have been applied for cyberattack classification because of their ability to learn nonlinear relationships within complex datasets [14]–[16]. These approaches demonstrate the potential of intelligent learning models for identifying abnormal behaviour in smart-grid communication and operational data.

Recent studies have focused on deep learning, ensemble learning, and hybrid architectures to improve detection performance. CNN-LSTM models have been investigated for extracting important features and capturing temporal dependencies in smart-grid data [17]. Ensemble and hybrid approaches have combined multiple classifiers or feature-learning techniques to improve robustness and reduce false alarms [18]–[20]. Other research has explored the combination of artificial intelligence with encryption, cyber-resilience mechanisms, and physics-based anomaly detection to provide more comprehensive protection for smart-grid systems [21]–[23]. These developments show a

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Volume 13, Issue 7, July 2026

clear transition from conventional detection techniques toward intelligent and adaptive cybersecurity solutions.

Although existing studies demonstrate promising detection performance, challenges remain in dataset diversity, false-alarm reduction, computational complexity, scalability, detection of changing attack patterns, and real-time implementation. Many approaches are primarily evaluated using datasets and software-based experiments, with comparatively less emphasis on practical low-cost hardware implementation. Therefore, there is a need for an intelligent detection system that combines effective attack classification with real-time monitoring. In this work, a Bilateral Convolutional Neural Network-based Artificial Neural Network (BCNN-ANN) approach is investigated for smart-grid cyberattack detection. MATLAB is used for data preprocessing, model training, classification, and performance evaluation, while Raspberry Pi 3B+ is used for real-time monitoring. The proposed system aims to provide an accessible approach for detecting cyberattacks and presenting the detected attack information through a graphical user interface and LCD display [24], [25].

Smart grids provide improved communication, automation, and monitoring capabilities, but their increased connectivity makes them vulnerable to cyberattacks such as DoS, false data injection, and unauthorized access. Existing research has explored machine learning, neural networks, deep learning, ensemble methods, and hybrid techniques for detecting such attacks. These methods have shown promising classification performance, but challenges remain in reducing false alarms, handling complex datasets, adapting to new attack patterns, and achieving real-time implementation. To address these limitations, the proposed work investigates a **BCNN-ANN-based intrusion detection approach** combined with **Raspberry Pi 3B+ deployment** for real-time smart-grid attack classification and monitoring.

III. PROPOSED METHODOLOGY

The proposed work develops a machine-learning-based intrusion detection system to identify abnormal activities in smart-grid communication networks. The network traffic dataset is first collected and preprocessed by converting categorical attributes into numerical features. Class balancing is performed to improve the detection of less frequent attacks. The dataset is then divided into training and testing sets to develop and compare Decision Tree, RUSBoost, ECOC Logistic Regression, ECOC Gaussian SVM, and Bi-lateral Neural Network models using accuracy, precision, recall, F1-score, confusion matrix, ROC curve, and AUC. The best-performing model is converted into deployable C code using MATLAB Coder and implemented on a Raspberry Pi 3B+ for real-time intrusion detection. The detected traffic class is displayed through a MATLAB App Designer interface and a 16×2 I²C LCD, with an alarm activated for abnormal traffic. Finally, Raspberry Pi predictions are compared with MATLAB results to verify system reliability.

BCNN-ANN Model:

A BNN-ANN model was developed for the classification of cybersecurity attacks in smart-grid communication data. The preprocessed dataset is supplied to the neural-network model, which learns the relationship between the input features and the corresponding traffic classes. The model performs multiclass classification of Normal, DoS, Probe, R2L, and U2R traffic.

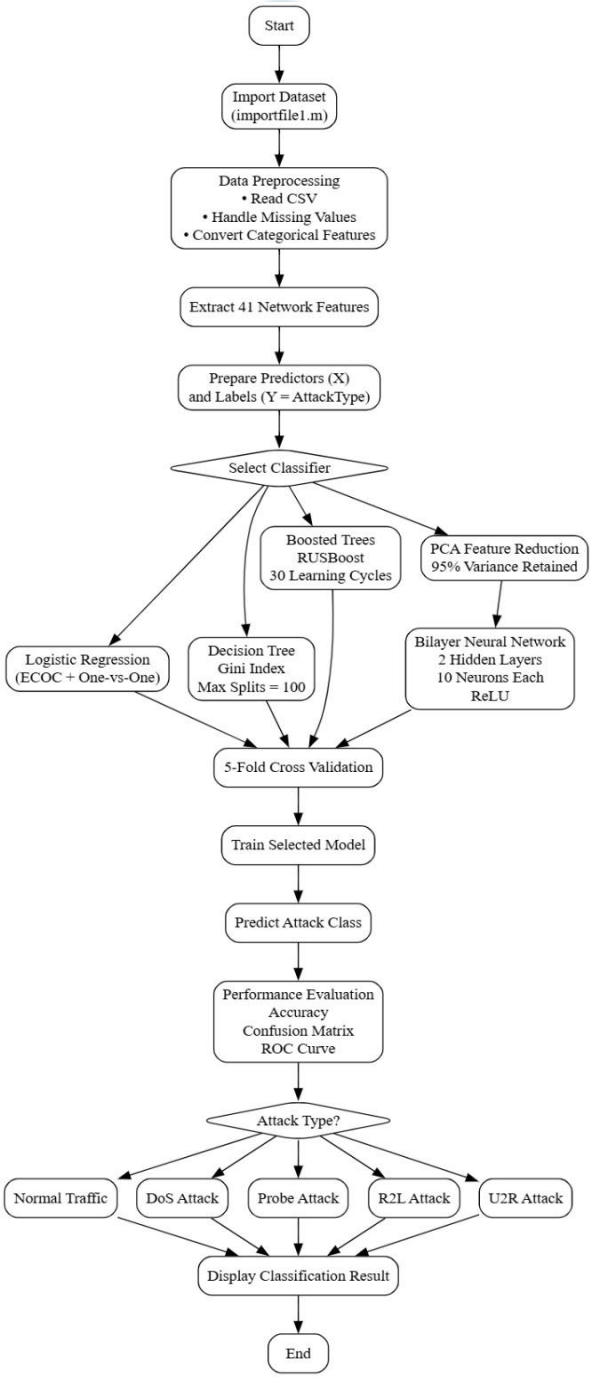


Fig.1. Flowchart of the proposed smart grid cyberattack detection

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Volume 13, Issue 7, July 2026

The neural-network model is trained in MATLAB using the Deep Learning Toolbox, and its performance is evaluated using accuracy, precision, recall, F1-score, confusion matrix, and ROC-AUC. The trained model is subsequently used for attack prediction in the proposed smart-grid cybersecurity detection system. The project report identifies the neural-network classifier as a two-hidden-layer neural network.

Training and Testing:

After preprocessing, the dataset was used for training and evaluation of the proposed machine learning models in MATLAB. The input data consisted of network traffic features corresponding to five classes: DoS, Normal, Probe, R2L, and U2R. Principal Component Analysis (PCA) was applied to the numerical features, retaining components that explained 95% of the total variance. The selected features were then provided to the classification models for training. For the neural-network-based model, a feed-forward neural network with two hidden layers was trained using the processed data. A 5-fold cross-validation technique was employed to validate the model by dividing the available data into five subsets, where four subsets were used for training and the remaining subset was used for validation in each iteration. The validation predictions from all five folds were combined to calculate the overall validation performance. The trained model was subsequently used to classify previously unseen network traffic during the testing and real-time prediction stage.

IV. BLOCK DIAGRAM

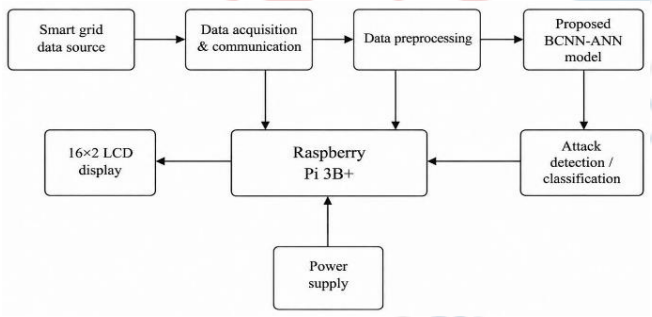


Fig.2. Block diagram

The block diagram shows the overall working of the proposed smart-grid cyberattack detection system. Initially, the network traffic data is prepared by removing unwanted information and converting the required features into a suitable format. Important features are then selected and the dataset is divided for model training and testing. The trained BCNN-ANN model learns the patterns of different network activities and identifies the type of traffic. The trained model is implemented on the Raspberry Pi 3B+ to perform real-time attack detection. Finally, the detected status is displayed on the MATLAB GUI and 16×2 LCD, helping the user monitor normal and malicious network activity.

V. IMPLEMENTATION OF SOFTWARE

The software implementation is carried out using MATLAB. The collected cybersecurity dataset is first preprocessed by handling categorical and numerical features, removing invalid values, reducing feature dimensionality using Principal Component Analysis (PCA), and standardizing the input features. The processed data is then used for training and testing the machine learning model. MATLAB Classification Learner and Deep Learning Toolbox are used for model development and evaluation. MATLAB App Designer is used to develop a graphical user interface for displaying the detection results. The trained model classifies the input data into normal traffic or different attack categories such as DoS, Probe, R2L, and U2R. The prediction obtained from the model is displayed through the GUI and 16×2 LCD, enabling real-time monitoring of cybersecurity threats in the smart grid environment.

MATLAB Classification Learner/Model

The preprocessed dataset was imported into MATLAB and used with the Classification Learner App for developing and evaluating machine learning classification models. The input features were provided to the Classification Learner, while the attack category was used as the response variable. The dataset was used to train the selected classification models for distinguishing between normal traffic and different types of cyberattacks. During model evaluation, cross-validation was used to assess the generalization performance of the trained models on unseen data. The trained model was evaluated using classification performance measures such as accuracy, confusion matrix, and ROC curve with AUC. The best-performing model was selected for further use in the proposed smart grid cybersecurity attack detection system.

MATLAB App Designer GUI

The developed system provides a MATLAB App Designer-based graphical user interface (GUI) for real-time cybersecurity analysis of smart-grid network traffic at the edge. The GUI establishes communication with a Raspberry Pi device and acquires network traffic features for intrusion detection. The extracted features are organized into four major categories: basic connection features, time-based traffic features, content-based features, and host-based traffic features.

The proposed interface enables the selection of a machine learning classifier and performs traffic classification directly using the Raspberry Pi edge device. Dataset samples can be loaded individually or selected randomly to evaluate the detection performance. The classification results display the predicted traffic category, confidence score, processing time, and class-wise prediction scores. In addition, the system supports an LCD status update and alarm activation when malicious traffic is detected.

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Volume 13, Issue 7, July 2026

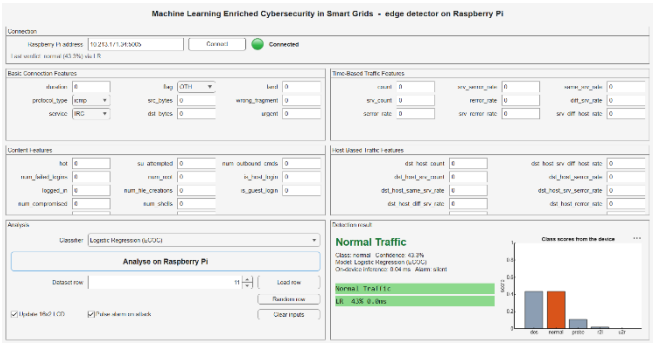


Fig.3. MATLAB App Designer GUI

VI. RESULT

The proposed machine learning-based cybersecurity attack detection system was evaluated using the preprocessed smart grid network dataset. The trained model successfully classified network traffic into different categories, including Normal, DoS, Probe, R2L, and U2R attacks. The performance of the model was evaluated using standard classification metrics such as accuracy, precision, recall, F1-score, confusion matrix, and ROC-AUC. The results demonstrate that the proposed system can effectively distinguish normal network activity from malicious traffic. The confusion matrix provides a detailed representation of correctly and incorrectly classified samples, while the ROC curve and AUC value indicate the model's ability to discriminate between different classes. The trained model was further integrated with the Raspberry Pi-based implementation, where the predicted attack category was displayed through the GUI and 16×2 LCD. These results demonstrate the feasibility of using machine learning for real-time cybersecurity attack detection in smart grid environments.

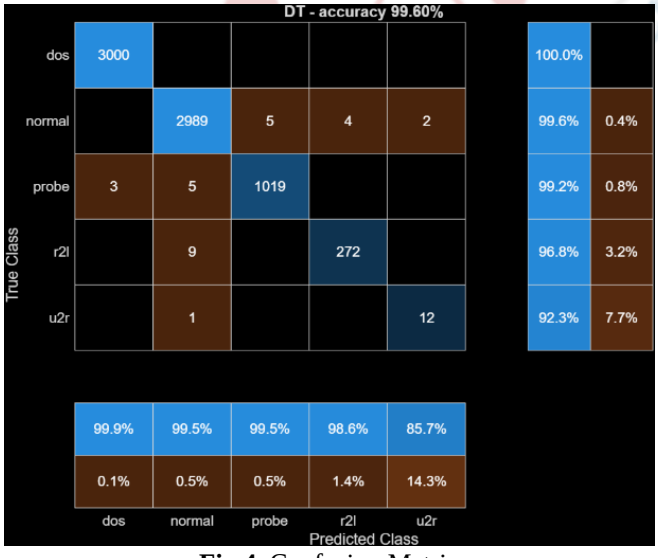


Fig.4. Confusion Matrix

The confusion matrix shows that the Decision Tree classifier correctly identifies most of the samples across the five traffic classes: DoS, Normal, Probe, R2L, and U2R. The model achieves an overall accuracy of **99.60%**, with **100% recall for DoS**, **99.6% for Normal**, **99.2% for Probe**, **96.8% for R2L**, and **92.3% for U2R**. Only a small number of samples are incorrectly classified, with more difficulty observed in the U2R class. These results indicate that the Decision Tree model can effectively distinguish normal network traffic from different types of cyberattacks.

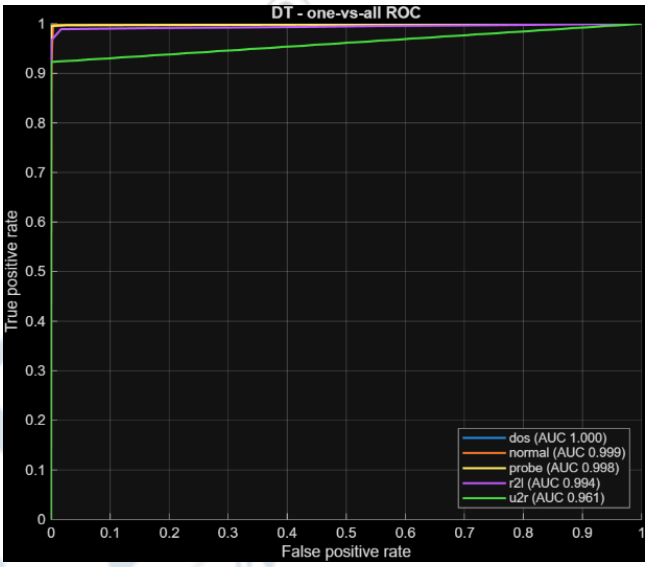


Fig.5. ROC Curve

The ROC curve further demonstrates the classification capability of the Decision Tree model for the five traffic categories. The AUC values obtained are **1.000 for DoS, 0.999 for Normal, 0.999 for Probe, 0.994 for R2L, and 0.961 for U2R**. The values close to 1 indicate that the classifier has a strong ability to separate the different traffic classes. DoS, Normal, and Probe show almost perfect discrimination, while U2R has a comparatively lower AUC, making it the more challenging class to identify. Overall, the ROC results confirm the reliable classification performance of the proposed model.

Comparison of Machine Learning Algorithms

Algorithms	Accuracy (%)
Decision Tree	99.60
Bi-lateral Neural Network	99.24
Binary Tree	98.17
SVM	97.81
Logistic Regression	81.40

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Volume 13, Issue 7, July 2026

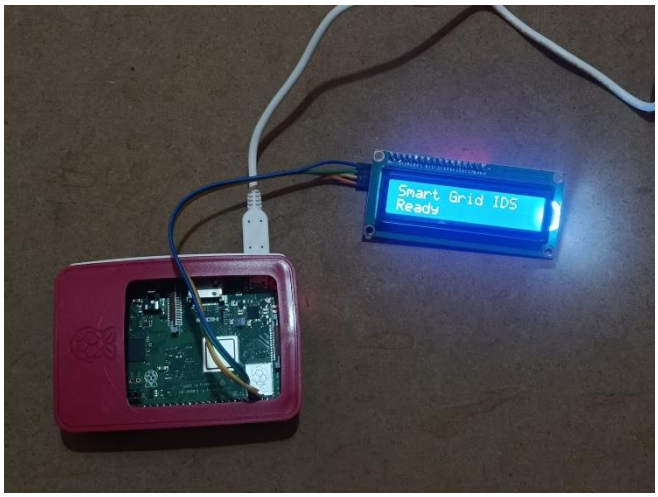


Fig.6. Initialization of the Proposed Smart Grid IDS

The developed smart grid intrusion detection system was implemented on a Raspberry Pi platform to demonstrate its capability for real-time cyberattack detection. As shown in the experimental setup, the Raspberry Pi is interfaced with a 16×2 LCD display, which provides the detection status directly to the user. The LCD initially displays **"Smart Grid IDS Ready"**, indicating that the system has been successfully initialized and is ready to process network traffic.



Fig.7. Real-time classification of normal traffic on the LCD.

During real-time operation, the system identifies the incoming traffic as **"Normal Traffic"** and displays **"LR 43%"** with a processing time of approximately **0.1ms**. Here, LR represents the Logistic Regression-based classification output used by the implemented detection system. The displayed result demonstrates that the trained model can perform traffic classification directly on the Raspberry Pi with very low computational delay. The approximately 0.1ms response time indicates the suitability of the proposed system for rapid traffic monitoring and real-time intrusion detection.

VII. CONCLUSION

This project presents a machine learning-based approach for detecting cybersecurity attacks in smart grid systems. The network data was preprocessed and classified using machine learning algorithms in MATLAB, with the Decision Tree model evaluated using performance measures such as accuracy, ROC curve, AUC, and confusion matrix. The results demonstrate that machine learning can effectively distinguish between normal and malicious network activities. A MATLAB App Designer GUI was developed to provide a user-friendly interface for displaying the predicted attack type. The proposed approach can enhance smart grid security by enabling faster and more reliable detection of cyber attacks and can be further improved by using larger real-time datasets and advanced machine learning techniques.

REFERENCES

[1] G. Amritha, M. G. Nair, and F. Granelli, "Machine Learning-Enriched Cybersecurity in Smart Grids," IEEE Access, vol. 13, pp. 99303–99313, Jun. 2025.

[2] A. Alsirhani, N. Tariq, M. Humayun, and H. Sanaullah, "Intrusion Detection in Smart Grids Using Artificial Intelligence-Based Ensemble Modelling," Cluster Computing, vol. 28, pp. 1–18, Feb. 2025.

[3] S. Tufail and H. Iqbal, "A Hybrid Machine Learning-Based Framework for Data Injection Attack Detection in Smart Grids Using PCA and Stacked Autoencoders," International Journal of Electrical Power and Energy Systems, vol. 162, pp. 1–12, 2025.

[4] M. A. Shahid and F. Ahmad, "Cyber-Resilient Smart Grids: A Randomized Coefficient-Based Defense Mechanism Against False Data Injection Attacks," Sustainable Energy Technologies and Assessments, vol. 68, pp. 1–10, 2025.

[5] Y. A. Farrukh, I. Khan, and Z. Ahmad, "A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System," IEEE NAPS Conference, pp. 1–6, 2021.

[6] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection," IEEE International Conference on Smart Energy Grid Engineering, pp. 108–112, Aug. 2019.

[7] S. Khan, K. Kifayat, A. K. Bashir, A. Gurtov, and M. Hassan, "Intelligent Intrusion Detection System in Smart Grid Using Computational Intelligence and Machine Learning," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, pp. 1–14, Jun. 2020.

[8] P. Haji Mirzaee, M. Shojafar, H. Cruickshank, and R. Tafazolli, "Smart Grid Security and Privacy: From Conventional to Machine Learning Issues," IEEE Access, vol. 10, pp. 52922–52954, 2022.

[9] M. M. Alani and T. Baker, "A Survey of Smart Grid Intrusion Detection Datasets," Intelligent Environments Conference, pp. 1–10, Jul. 2023.

[10] M. Ravinder and V. K. Kulkarni, "Intrusion Detection in Smart Meter Data Using Machine Learning," Frontiers in Energy Research, vol. 11, pp. 1–9, Feb. 2023.

[11] A. Subasi, E. Alickovic, and J. Kevric, "Intrusion Detection in Smart Grid Using Data Mining Techniques," Saudi Computer Society National Computer Conference, pp. 1–6, Apr. 2018.

[12] M. N. Kurt, O. Ogundijo, and X. Wang, "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach," IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5174–5185, 2019.

[13] Ö. Sen, D. van der Velde, et al., “On Specification-Based Cyber-Attack Detection in Smart Grids,” arXiv, pp. 1–12, 2022.
[14] H. Patel and S. Nair, “Artificial Intelligence Techniques for Smart Grid Protection,” International Journal of Power Electronics, vol. 18, no. 5, pp. 101–110, 2022.
[15] R. Joseph and A. Thomas, “Cybersecurity Enhancement in Smart Grid Using Artificial Neural Networks,” Journal of Electrical Systems, vol. 16, no. 3, pp. 220–228, 2020.
[16] M. Amin, “Importance of Security for the Smart Grid,” IEEE Smart Grid, pp. 1–8, 2021.
[17] A. Alsaiari and M. Ilyas, “Deep Learning for Smart Grid Intrusion Detection: A Hybrid CNN-LSTM-Based Model,” International Journal of Artificial Intelligence Applications, vol. 15, no. 3, pp. 1–16, May 2024.
[18] T. Gupta and R. Bhatia, “False Data Injection Attack Detection in Smart Grid Framework,” 2024.
[19] A. Alsirhani, N. Tariq, M. Humayun, and H. Sanaullah, “Intrusion Detection in Smart Grids Using Artificial Intelligence-Based Ensemble Modelling,” Cluster Computing, vol. 28, pp. 1–18, Feb. 2025.
[20] S. Tufail and H. Iqbal, “A Hybrid Machine Learning-Based Framework for Data Injection Attack Detection in Smart Grids Using PCA and Stacked Autoencoders,” International Journal of Electrical Power and Energy Systems, vol. 162, pp. 1–12, 2025.
[21] M. A. Shahid and F. Ahmad, “Cyber-Resilient Smart Grids: A Randomized Coefficient-Based Defense Mechanism Against False Data Injection Attacks,” Sustainable Energy Technologies and Assessments, vol. 68, pp. 1–10, 2025.
[22] Y. Y. Ghadi and T. Mazhar, “A Hybrid AI-Blockchain Security Framework for Smart Grids,” 2025.
[23] G. Amritha, M. G. Nair, and F. Granelli, “Machine Learning-Enriched Cybersecurity in Smart Grids,” IEEE Access, vol. 13, pp. 99303–99313, Jun. 2025.
[24] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–Physical System Security for the Electric Power Grid,” Proceedings of the IEEE, vol. 100, no. 1, pp. 210–224, Jan. 2017.
[25] K. Moslehi and R. Kumar, “Smart Grid Security: Threats, Challenges and Solutions,” Electric Power Systems Research, vol. 149, pp. 1–10, 2017.