e-ISSN: 3027-0650
Vol. 2, Issue 1, pp262-270, November 6 -9, 2024

Comparative Analysis of Machine Learning Models for Enhancing Cybersecurity on Cyber-physical Systems in Smart Grids Against DDoS Attacks

Idowu Afe[1], Idris Ismaila[2], Ojeniyi Joseph Adebayo[3] , Abdullahi Raji Egigogo[4]
{Afeidowu@gmail.com[1], ismi.idris@futminna.edu.ng[2], ojeniyija@futminna.edu.ng[3] and rajiaegigogo@auk.edu.ng}
Federal Universiy of Technology Minna[1234]

Abstract. Detecting Distributed Denial of Service (DDoS) attacks in cyber-physical systems, particularly smart grids, requires highly accurate and efficient solutions. This study evaluates the performance of several machine learning algorithms, including Logistic Regression, Naive Bayes, K-Nearest Neighbors, Decision Trees, Support Vector Machine, Random Forest, Gradient Boosting Machines, XGBoost, Artificial Neural Networks, and Recurrent Neural Networks for detecting DDoS attacks. The CICIDS2017 dataset, which includes real-world attack scenarios, was used for training and testing. The evaluation metrics, such as precision, recall, accuracy, and F1-score, demonstrate exceptional performance across most algorithms, with XGBoost achieving perfect scores on all metrics. Other models, such as RF, DT, and GBM, also show near-perfect performance, while simpler models like Naive Bayes, though slightly lower, still provide viable detection capabilities. These results emphasized the importance of advanced machine learning algorithms in ensuring the security and stability of critical infrastructure like smart grids.

Keywords: Cyber-physical Systems, DDoS, Machine Learning, Smart Grids

1 Introduction

Smart grids are a vital component of modern cyber-physical systems (CPS). They integrate information and communication technology (ICT) into electrical power networks, ensuring efficient and reliable energy distribution [1]. However, this convergence of digital and physical systems also introduces vulnerabilities, particularly in cyberattacks such as Distributed Denial of Service (DDoS) [2]. A DDoS attack aims to overwhelm communication networks or services by flooding them with excessive traffic, thereby disrupting normal operations [3].
Machine learning (ML) models offer significant potential for detecting these attacks by identifying patterns and anomalies within network traffic data [4]. The critical challenge is selecting and evaluating the most effective classification algorithms that can function in real time and accurately detect DDoS attacks without compromising the smart grid's performance [5].

In this paper, we present an experimental analysis of ten machine-learning classification algorithms used for DDoS detection on cyber-physical system in smart grids. These algorithms were evaluated based on crucial performance metrics: precision, recall, accuracy, and F1-score. The primary objective is to identify the most effective algorithm for enhancing DDoS detection and strengthening the cyber-physical system security in smart grid.

2 Related Work

This review assesses various studies on cyber-physical systems (CPS) and smart grid environments, focusing on detecting and mitigating Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks using a range of machine learning and statistical techniques.

[6] combined rule-based and machine-learning methods for detecting DDoS attacks in CPPS, achieving a weighted accuracy of 98.71% and real-time solid performance. Future research is needed to extend its applicability to broader contexts.

[7] introduced a Hierarchical Bayesian Network (HBN) model enhanced by bacterial foraging optimization (BFO) to defend CPS against DoS attacks. The model achieved high accuracy (98.4%) and low RMSE (0.0617), demonstrating scalability for large-scale CPS. However, its computational demands are a significant limitation.

[8] proposed a hybrid machine-learning technique for detecting DDoS attacks in smart grids. The technique achieves 83.23% accuracy with moderate precision, recall, and F1-score. Despite its novel approach, the model requires substantial improvements in precision and recall.

[9] used Decision Tree, Random Forest, K-Nearest Neighbors and PCA for DDoS detection in Industry 4.0 CPPS, achieving near-perfect accuracy and F1-scores. The study highlighted the superior performance of supervised models but noted challenges in unsupervised learning.

[10] proposed a sequential supervised machine learning approach using a two-layer hierarchical Random Forest Classifier (RFC) for cyber-attack detection in smart grids. The model achieved 95.44% accuracy, effectively handling data imbalance and feature reduction, but preprocessing improvements are necessary.

[11] explored ensemble learning methods for anomaly detection in smart grids, with stacking-based ensembles achieving the highest accuracy (97.3%). Despite their effectiveness, the models' complexity and varying performance across methods pose challenges.

[12] developed a machine learning-based detection model for DoS attacks in smart grids, employing SVM, Decision Tree, and Naive Bayes classifiers. The model showed strong performance with precision, recall, and F1-score all at 0.97, though further refinement is needed.

[13] focused on enhancing SCADA system security against DDoS attacks using Naive Bayes, J48 and Random Forest algorithms. Random Forest showed the highest accuracy (99.99%), but the study's reliance on the KDDCup'99 dataset limits its real-world relevance.

[14] applied shallow and deep auto-encoders with Multiple Kernel Learning (MKL) for DDoS detection in smart grids, achieving high accuracy (97%) and robust feature learning. The model outperformed state-of-the-art methods but requires optimization for larger datasets.

[15] proposed an intrusion detection system using data mining techniques, achieving high accuracy (98.94%) and an AUC of 0.999. However, the study does not address the computational costs or complexity of the approach.

3.Methodology

3.1 Dataset

The dataset used for the evaluation is CICIDS2017, which was due to its extensive range of current attack scenarios, which meet real-world conditions and are widely available and used in the cybersecurity community. Furthermore, it includes results from CICFlowMeter network traffic analysis, with flows categorized by source, timestamp, destination IP addresses, destination ports, protocols, and attack types [16], [5].

Table 1: Database Description

Dataset	Total number of features	BENIGN	DDoS	Total
CICIDS2017	78	97718	128027	225745

3.2 Experimental Evaluation and Metrics

The algorithms were implemented through experimentation in Google Colab using Python code with the CICIDS2017 cyber security dataset. The models are evaluated using the following metrics [18], [19].

Accuracy: The proportion of correctly classified instances.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}} = + \frac{\text{True Positive}}{\text{Total Predicted Positive}} \quad (1)$$

Precision: The ability of the classifier to avoid false positives.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} = + \frac{\text{True Positive}}{\text{Total Predicted Positive}} \quad (2)$$

Recall: The ability of the classifier to detect all true positives.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} = + \frac{\text{True Positive}}{\text{Total Predicted Positive}} \quad (3)$$

F1-Score: The harmonic mean of precision and recall, providing a balance between the two.

$$\text{F1} - \text{score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} = + \frac{\text{True Positive}}{\text{Total Predicted Positive}} \quad (4)$$

3.3 Model Training and Testing

The data was split into training (80%) and validation/testing (20%) sets, ensuring a balanced model training and evaluation approach. The models are trained using the training data and evaluated using the testing data.

3.4 Feature Selection

In this critical phase of the machine learning process, the focus was on data preprocessing and feature selection to optimize model performance and predictive accuracy. The process began with identifying and engineering key features that significantly impact resilience, ensuring they effectively capture the relationships within the dataset. Data cleaning

was the first step, replacing NaN and infinite values with the mean of the respective columns. Next, features were converted to numerical values using a standard scaler, as shown in equation 5, while labels were encoded, with benign represented as 0 and DDoS as 1 using equation 6. The dataset was then normalized to a uniform range of [0, 1] to reduce feature discrepancies.

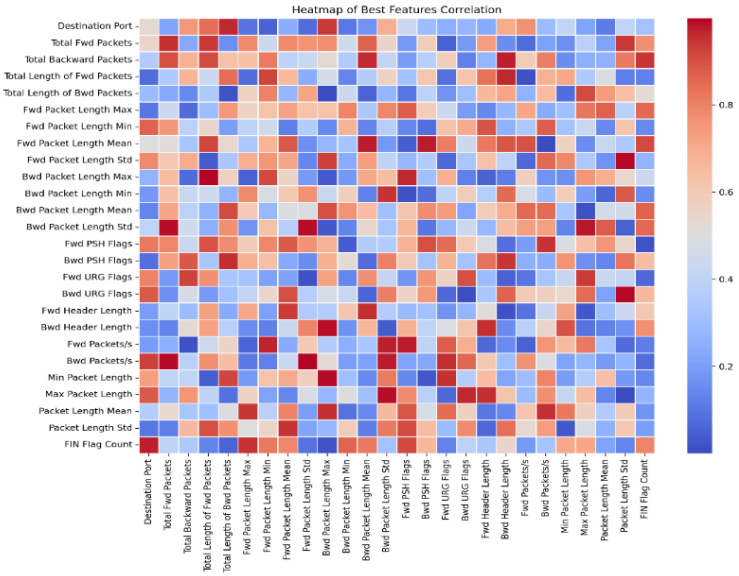

Fig 1: Heatmap of the best features in the Dataset

$$\sigma = \sqrt{\sum_{i=1}^{n}(xi - \mu)^2} \quad (5)$$

$$z = f(x) = \sigma\,(\mathrm{W}e^{x} + b_e) \quad (6)$$

In this paper, ten (10) machine-learning classification algorithms for the detection of DDoS attack on cyber-physical systems were evaluated through experimentation. The algorithms are discussed as follows [20], [21].

i. Random Forest: This is an ensemble learning technique that creates multiple decision trees and combines their outputs to enhance accuracy in classification or regression tasks. It is resistant to overfitting and performs well with noisy data.

ii. Support Vector Machine (SVM): A powerful classification algorithm that finds the best hyperplane to divide data points into distinct classes. SVMs are effective in high-dimensional spaces and can handle both linear and non-linear data using kernel functions.

iii. K-Nearest Neighbors (KNN): An instance-based learning algorithm that classifies data points by considering the majority class among their nearest 'k' neighbors. Although simple and intuitive, KNN can be computationally demanding with large datasets.

iv. Decision Trees: These models split data based on feature values, forming a tree-like structure where each node represents a decision rule, and each leaf node represents an outcome. They are easy to understand but can overfit if not appropriately pruned..

v. Artificial Neural Networks (ANNs): Inspired by the human brain, these computational models consist of layers of interconnected neurons. ANNs can learn complex patterns in data and are fundamental to deep learning, though they require large amounts of data and significant computational power.

vi. Naive Bayes: A probabilistic classifier that applies Bayes' theorem with the assumption of feature independence. Despite this simplification, it performs effectively in tasks like text classification, where the assumption approximately holds.

vii. Gradient Boosting Machines (GBM): An ensemble method that sequentially builds models, with each new model aimed at correcting the errors of its predecessors. By combining weak learners, typically decision trees, GBMs create a robust predictive model that often yields high accuracy.

viii. Logistic Regression: A linear model for binary classification that estimates the likelihood of a particular outcome based on input features. It is simple, interpretable, and effective when the relationship between variables and the outcome is roughly linear.

ix. Extreme Gradient Boosting (XGBoost): A refined version of gradient boosting that is highly efficient and scalable. XGBoost is known for its speed and accuracy, making it a popular choice in machine learning competitions, especially for large datasets.

x. Recurrent Neural Networks (RNNs): These neural networks are designed for sequential data, with connections that form directed cycles. RNNs are particularly suitable for tasks like time series analysis and natural language processing but may encounter difficulties with long-term dependencies due to issues such as vanishing gradients. The detection framework of the DdoS attack using ten diffirent alogorithm is illustred in Figure 2.

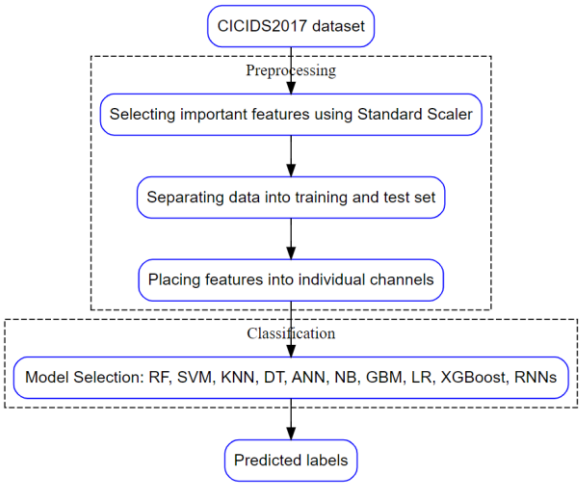

Fig 2: DDoS Detection Framework

4. Results

The performance of each machine learning model is summarized in Table 2

Algorithms	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
Random Forest	99.99	99.99	99.99	99.99
SVM	99.86	99.86	99.86	99.86
XGBOOST	100.00	100.00	100.00	100.00
Logistic Regression	99.82	99.82	99.82	99.82
GBM	99.98	99.98	99.98	99.98
Naive Bayes	98.73	98.75	98.73	98.72
Decision Tree	99.99	99.99	99.99	99.99
KNN	99.98	99.98	99.98	99.98
ANN	99.91	99.91	99.91	99.91
RNN	99.86	99.86	99.86	99.86

The results on Table 2 reveal exceptionally high performance across various machine learning algorithms, with accuracy, precision, recall, and F1 scores consistently exceeding 98%. XGBoost stands out with perfect scores of 100% across all metrics, indicating flawless performance, likely due to its advanced boosting techniques that effectively minimize errors. RF, DT, and GBM also show near-perfect results, with scores of 99.99%, underscoring their robustness and effectiveness in handling complex datasets. ANNs, SVM and RNNs exhibit robust and consistent performance, each achieving 99.86% across all metrics, reflecting their capability to model intricate relationships within data KNN and LR also deliver excellent outcomes, with scores of 99.98% and 99.82%, respectively. While Naive Bayes lags slightly behind the others, with scores around 98.73%, it still performs commendably, given its simplicity and the assumption of feature independence. Overall, these results highlight the exceptional capability of each algorithm, with XGBoost, RF, and GBM leading in performance and even the slightly lower-scoring NB remaining a viable option. Figure 3 depicts the comparison of the algorithms. Confusion Matrix(CM) and Receiver Operating Characteristics (ROC) is presented in Figure 4 to 22 respectively.

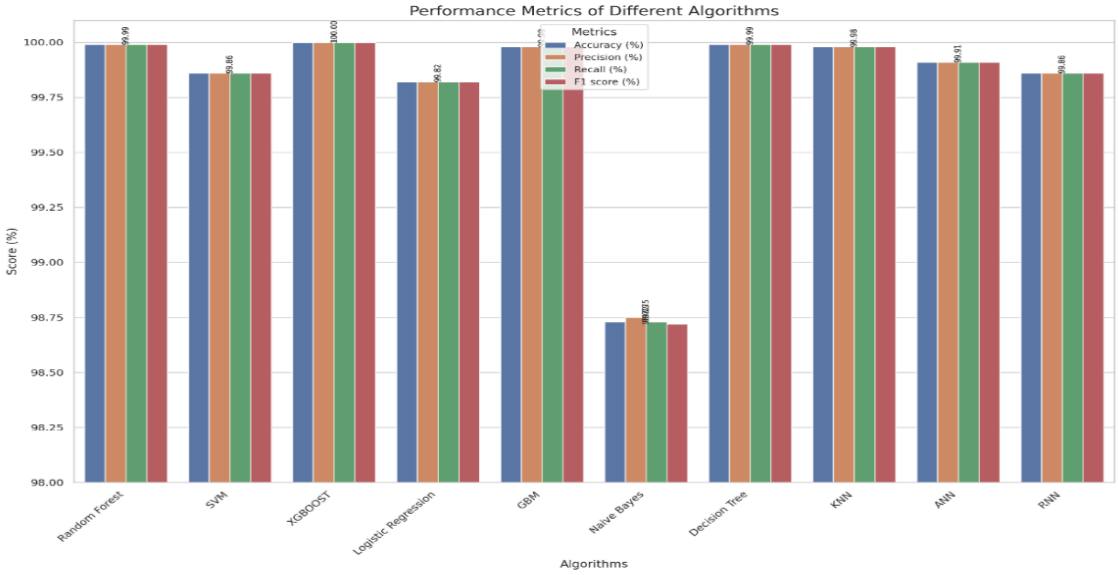

Fig 3. Comparisons of the performance of Machine Learning Algorithms

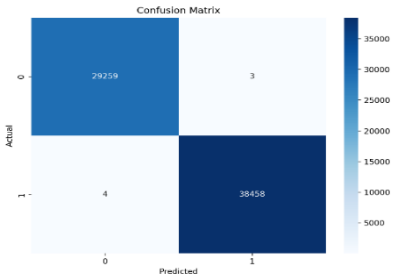

Fig 4: CM of RM Algorithm

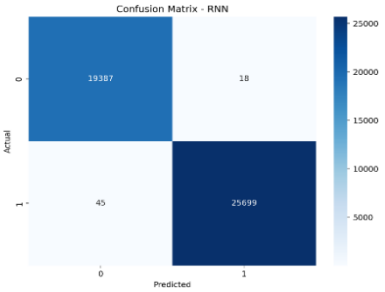

Fig 5: CM of RNN Algorithm

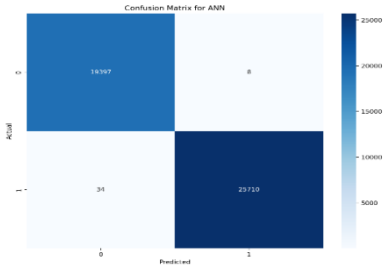

Fig 6: CM of ANN Algorithm

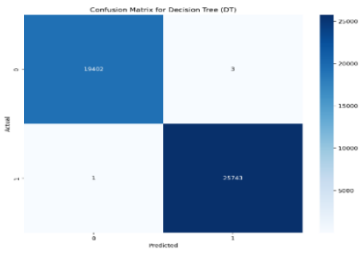

Fig7: CM of DT Algorithm

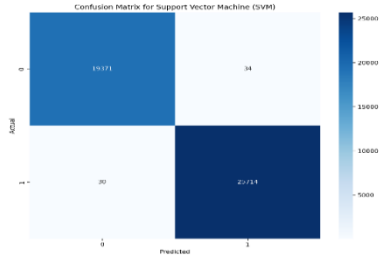

Fig. 8: CM of SVM Algorithm

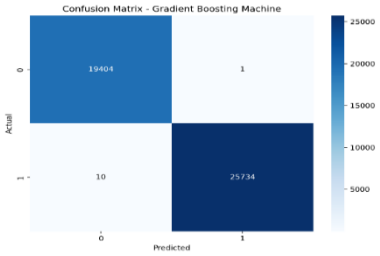

Fig 9: CM of GBM Algorithm

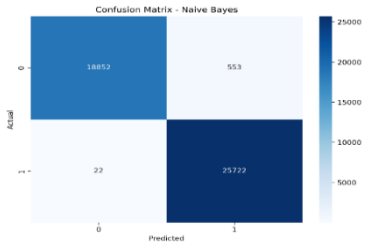

Fig 10: CM of NB Algorithm

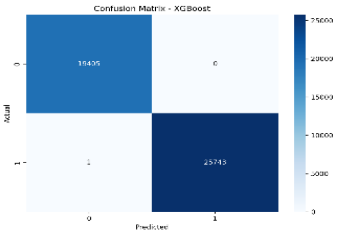

Fig 11: CM of XGB Algorithm

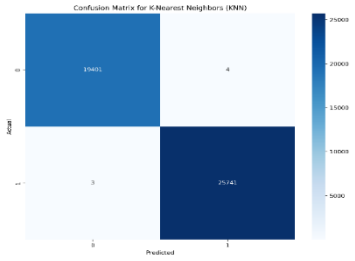

Fig 12: CM of KNN Algorithm

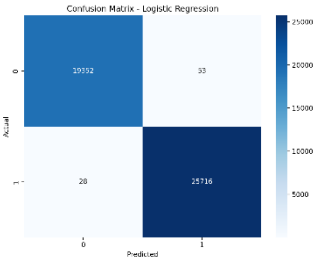

Fig 13: CM of LR Algorithm

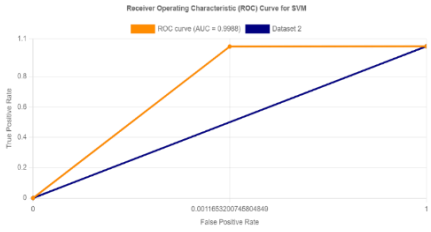

Fig 14: ROC of SVM Algorithm

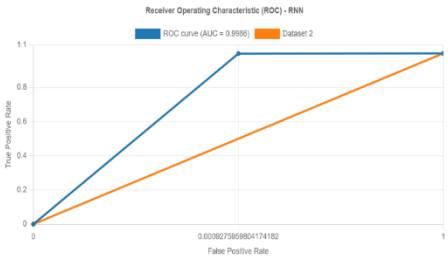

Fig 15: ROC of RNN Algorithm

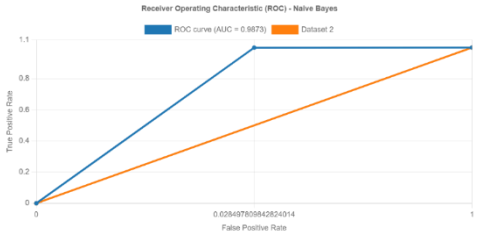

Fig 16: ROC of NB Algorithm

Fig 17: ROC of XGB Algorithm

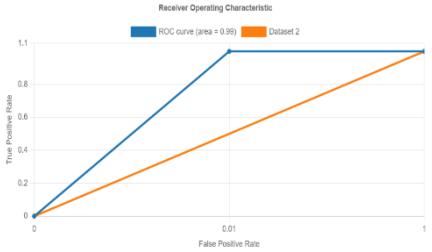

Fig 18: ROC of RF Algorithm

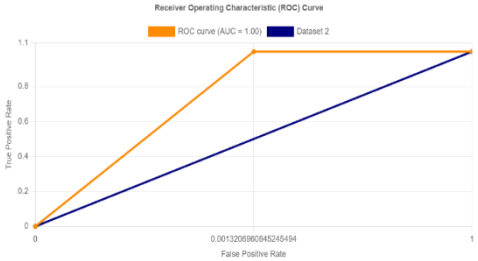

Fig 19: ROC of KNN Algorithm

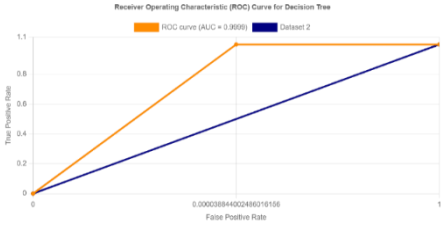

Fig 20: ROC of DT Algorithm

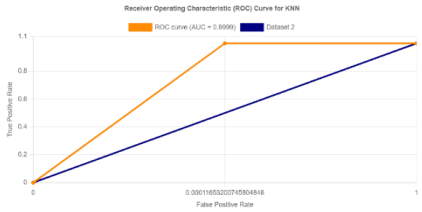

Fig 21: ROC of ANN Algorithm

Fig 22: ROC of LR Algorithm

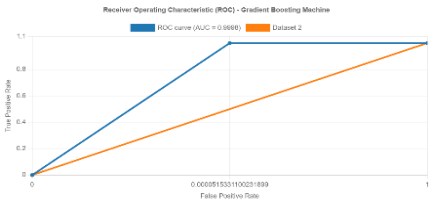

Fig 23: ROC of GBM Algorithm

6. Discussion

This study comprehensively evaluates various machine learning algorithms for detecting DDoS attacks in cyber-physical systems, especially smart grids. Most algorithms performed exceptionally well, with accuracy, precision, recall, and F1 scores exceeding 98%. XGBoost achieved perfect scores across all metrics, demonstrating flawless detection capabilities. Random Forest, Decision Trees, and GBM also showed near-perfect results at 99.99%, highlighting their robustness. SVM, ANNs, and RNNs followed closely with 99.86%, while KNN and Logistic Regression achieved 99.98% and 99.82%, respectively. Although Naive Bayes performed slightly lower at 98.73%, it remained a viable option due to its simplicity. The study emphasizes the effectiveness of advanced algorithms, particularly XGBoost, RF, and GBM, for real-time DDoS detection in smart grids.

7. **Conclusion**

This study evaluates various machine learning algorithms for detecting DDoS attacks on cyber-physical system in smart grids, showing that most achieved over 99% accuracy, precision, recall, and F1-score. XGBoost was the top performer with flawless detection, while Random Forest, Decision Trees, and Gradient Boosting Machines also demonstrated near-perfect results. Simpler models like Naive Bayes performed slightly lower but remained effective in specific contexts. The study underscores the crucial role of machine learning in ensuring the security of cyber-physical systems. It suggests future research focus on integrating these models into real-time detection systems for enhanced practical application.

References

[1] M. K. Hasan, A. K. M. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," *Energy Reports*, vol. 9, pp. 1318–1326, 2023, doi: https://doi.org/10.1016/j.egyr.2023.05.184.

[2] M. Snehi and A. Bhandari, "Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks," *Computer Science Review*, vol. 40, 2021, doi: 10.1016/j.cosrev.2021.100371.

[3] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System Over 5G Network," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, vol. 17, no. 2, pp. 860–870, 2021, doi: 10.1109/TII.2020.2974520.

[4] M. Shafiq, S. Nazir, and X. Yu, "Identification of Attack Traffic Using Machine Learning in Smart IoT Networks," *SECURITY AND COMMUNICATION NETWORKS*, vol. 2022, 2022, doi: 10.1155/2022/9804596.

[5] A. Aribisala, M. S. Khan, and G. Husari, "MACHINE LEARNING ALGORITHMS AND THEIR APPLICATIONS IN CLASSIFYING CYBER-ATTACKS ON A SMART GRID NETWORK," in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2021, pp. 63–69. doi: 10.1109/IEMCON53756.2021.9623067.

[6] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-based with Machine learning IDS for DDoS attack detection in cyber-physical production systems (CPPS)," *IEEE Access*, vol. 12, no. July, 2024, doi: 10.1109/ACCESS.2024.3445261.

[7] A. M. Ma, X., Almutairi, L., Alwakeel, "Cyber Physical System for Distributed Network Using DoS Based Hierarchical Bayesian Network," *Grid Computing*, 2023, doi: 10.1007/s10723-023-09662-1.

[8] A. K. M. A. Habib, M. K. Hasan, R. Hassan, S. Islam, R. Thakkar, and N. Vo, "Distributed denial-of-service attack detection for smart grid wide area measurement system: A hybrid machine learning technique," *Energy Reports*, vol. 9, pp. 638–646, 2023, doi: 10.1016/j.egyr.2023.05.087.

[9] F. B. Saghezchi, G. Mantas, M. A. Violas, A. M. de Oliveira Duarte, and J. Rodriguez, "Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs," *ELECTRONICS*, vol. 11, no. 4, 2022, doi: 10.3390/electronics11040602.

[10] Y. A. Farrukh, Z. Ahmad, I. Khan, and R. M. Elavarasan, "A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System," in *2021 North American Power Symposium (NAPS)*, 2021, pp. 1–6. doi: 10.1109/NAPS52732.2021.9654767.

[11] T. T. Khoei, G. Aissou, W. C. Hu, and N. Kaabouch, "Ensemble Learning Methods for Anomaly Intrusion Detection System in Smart Grid," in *2021 IEEE International Conference on Electro Information Technology (EIT)*, 2021, pp. 129–135. doi: 10.1109/EIT51626.2021.9491891.

[12] W. Zhe, C. Wei, and L. Chunlin, "DoS attack detection model of smart grid based on machine learning method," in *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, 2020, pp. 735–738. doi: 10.1109/ICPICS50287.2020.9202401.

[13] F. A. Alhaidari and E. M. AL-Dahasi, "New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, 2019, pp. 1–6. doi: 10.1109/ICCISci.2019.8716432.

[14] S. Ali and Y. Li, "Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network," *IEEE Access*, vol. 7, pp. 108647–108659, 2019, doi: 10.1109/ACCESS.2019.2933304.

[15] M. A.-N. Subasi, A. S., Khloud Al-Marwani, R. A, Kwairanga, A. Saeed M. Q. and K. A. R., "Intrusion Detection in Smart Grid Using Data Mining Techniques," 2018, doi: http://dx.doi.org/10.1109/NCG.2018.8593124.

[16] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, vol. 2018-Janua, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[17] F. Dehghan, "A Deep Learning-Based Method for Intrusion Detection in Smart Grid: A Case Study of Distributed Denial of Service Detection," *2024 28th International Electrical Power Distribution Conference, EPDC 2024*, 2024, doi: 10.1109/EPDC62178.2024.10571748.

[18] S. Y. Diaba and M. Elmusrati, "Proposed algorithm for smart grid DDoS detection based on deep learning," *Neural Networks*, vol. 159, pp. 175–184, 2023, doi: 10.1016/j.neunet.2022.12.011.

[19] Adejimi, Sodiya, Ojesanmi, Falana, and Tinubu, “A dynamic intrusion detection system for critical information infrastructure,” *Scientific African*, vol. 21, no. August, p. e01817, 2023, doi: 10.1016/j.sciaf.2023.e01817.
[20] Q. Ling, “Machine learning algorithms review,” vol. 0, pp. 91–98, 2023, doi: 10.54254/2755-2721/4/20230355.
[21] P. P. Rajani Rajalingam, Madhusudhana Reddy Barusu, Prathibha Priyadarshini, “Machine learning algorithms,” vol. 2, pp. 244–250, 2022.