Threat-Aware Intrusion Detection and Prevention for IEDs in Smart Grids Using Edge Computing and Hybrid ML Models

GUNTHA BHARGAV BALAJI

KL University, bhargavbalajiguntha@gmail.com

Abstract: An edge computing-based and threat behavior-aware smart prioritization framework is designed for cybersecurity intrusion detection and prevention in intelligent electronic devices (IEDs) within smart grids. Using the Power System Intrusion Detection dataset, various machine learning algorithms, including SVM, One-Class SVM, Gradient Boosting, LightGBM, Random Forest, and a Stacking Classifier combining Random Forest, LightGBM, and ExtraTreesClassifier, are employed for binary and multi-class intrusion detection tasks. The framework leverages the integration of modified LightGBM and One-Class SVM models to enhance detection accuracy and adaptability to evolving threats. Results demonstrate that the Stacking Classifier achieves the highest performance, with an accuracy of 99.5% in binary classification and 87.2% in multi-class classification. By leveraging the strengths of individual models and optimizing their integration, the proposed framework significantly improves the accuracy and reliability of intrusion detection systems in smart grids, ensuring robust and efficient cybersecurity. This approach is particularly effective in identifying complex threat behaviors, prioritizing critical alerts, and enabling real-time prevention mechanisms within the edge computing paradigm.

"Index Terms - *Edge Computing, Intrusion Detection, Smart Grids, Stacking Classifier, Cybersecurity, Threat Behavior Analysis".*

1. INTRODUCTION

The ‘‘smart grid environment’’ represents a significant shift from traditional electrical supply networks, offering a more sustainable, reliable, and efficient infrastructure. This modernized grid integrates a wide range of innovative components such as intelligent electronic devices (IEDs), communication networks, control systems, and data analytics tools to enhance the management, distribution, and consumption of electricity. The evolution of smart grids is driven by the need to address challenges such as growing electricity demand, renewable energy integration, and the need for improved energy efficiency in a rapidly changing environment [1].

The role of intelligent electronic devices (IEDs) within smart grids cannot be overstated, as they are key elements that enable advanced functionalities like remote monitoring, real-time control, and automated responses to grid anomalies. IEDs, in conjunction with advanced communication networks, ensure that information flows seamlessly between various components of the grid, thus improving the overall reliability and security of the energy infrastructure [2]. These devices also facilitate the integration of renewable energy sources, such as solar and wind, by dynamically managing power generation and distribution based on real-time grid conditions. As a result, energy storage systems and smart meters have become integral parts of this advanced ecosystem, further boosting the efficiency and sustainability of smart grids [3][4].

Machine learning (ML) technologies play a vital role in optimizing the operation and management of smart grids, particularly in energy storage systems, power management, and load forecasting. ML

models are employed to predict energy consumption patterns, detect anomalies, and optimize power generation from renewable sources. Recent advancements in hybrid machine learning models have proven to be highly effective in enhancing energy prediction accuracy, making them indispensable tools for managing the complexities of smart grids [5][6]. Machine learning also aids in optimizing energy consumption, minimizing waste, and improving grid resilience by identifying and responding to potential threats in real-time [7].

The integration of these technologies is not without challenges, particularly in terms of cybersecurity. With the increasing complexity of smart grids, ensuring the security of IEDs, communication networks, and control systems becomes a critical concern. Therefore, robust intrusion detection and prevention systems are essential to protect against cyber threats. By leveraging advanced ML algorithms such as Support Vector Machines (SVM), One-Class SVM, Gradient Boosting, and LightGBM, as well as combining them in ensemble models like Stacking Classifiers, smart grids can effectively identify and mitigate cyber threats, ensuring the integrity of the entire system [2][3]. Through this combination of cutting-edge technologies, the smart grid of the future is expected to be more efficient, resilient, and secure, paving the way for a more sustainable energy landscape.

2. RELATED WORK

The integration of machine learning and cybersecurity in smart grids has been the focus of various studies, highlighting innovative approaches to address the increasing complexity of modern energy systems. Wang et al. [8] introduced a stacking ensemble GRU optimization algorithm using a federated learning framework to detect cyberattacks, specifically electricity theft, in smart grids. Their approach ensures data privacy while enhancing detection accuracy by leveraging distributed data learning. Li et al. [9] proposed an adaptive deep learning neural network model to improve machine learning-based classifiers for intrusion detection in smart grids, showcasing its adaptability to dynamic network conditions. Similarly, Yu et al. [10] developed an advanced and accurate intrusion detection system based on evolving machine learning techniques, emphasizing real-time detection and adaptability to evolving cyber threats in smart grids.

Zhukabayeva et al. [11] presented a traffic analysis and node categorization-aware framework that integrates machine learning to enhance intrusion detection and prevention for wireless sensor networks (WSNs) in smart grids. This framework focuses on traffic pattern recognition to detect malicious nodes effectively. Mhmood et al. [12] introduced an improved VGG19 deep neural network architecture combined with the Aquila optimizer algorithm for cyber-attack detection, achieving high accuracy in identifying complex attack patterns in smart grids. Zhao et al. [13] enhanced intrusion detection for asset integrity management (AIM) in smart grids by proposing a novel detection method tailored to the unique requirements of AIM, ensuring better system security and reliability.

Alani et al. [14] proposed a two-stage cyberattack detection and classification system for smart grids, where the first stage identifies potential attacks, and the second stage classifies them into specific categories, improving response times and accuracy. Panthi and Das [15] developed an intelligent intrusion detection scheme using optimized ensemble learning on selected features, effectively reducing computational overhead while maintaining high detection accuracy. These approaches

underline the critical role of feature selection and ensemble methods in enhancing intrusion detection performance.

Together, these studies demonstrate the potential of machine learning, deep learning, and ensemble methods in addressing cybersecurity challenges in smart grids. They highlight the need for adaptive, scalable, and efficient frameworks capable of handling dynamic and evolving threats while ensuring system reliability and data integrity in the increasingly interconnected energy landscape.

3. MATERIALS AND METHODS

The proposed system introduces a smart prioritization framework for intrusion detection and prevention in intelligent electronic devices (IEDs) within smart grids, leveraging edge computing and advanced machine learning techniques [8][9][11]. Utilizing the Power System Intrusion Detection dataset, the system integrates multiple algorithms, including SVM, One-Class SVM, Gradient Boosting, LightGBM, and a Stacking Classifier that combines Random Forest, LightGBM, and ExtraTreesClassifier [8][10][12]. The system aims to enhance detection accuracy and threat behavior analysis by combining the strengths of individual algorithms and optimizing their performance for both binary and multi-class classification tasks [9][13][14]. This approach ensures efficient and reliable identification of cyber threats, enabling real-time prevention and improved security in smart grid environments [15].

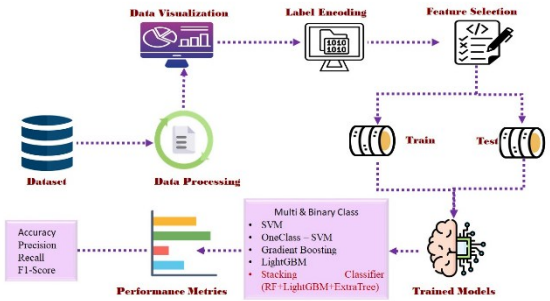


Fig.1 Proposed Architecture

The image (Fig.1) This cybersecurity intrusion detection and prevention system for smart grids leverages edge computing and threat behavior analysis. The system starts with data collection and preprocessing, which includes data visualization, label encoding, and feature selection. The preprocessed data is then split into training and testing sets. A combination of machine learning models, including SVM, One-Class SVM, Gradient Boosting, LightGBM, and a stacking classifier, is trained and tested on the data. The system evaluates model performance using metrics like accuracy, precision, recall, and F1-score to identify the most effective intrusion detection approach.

i) Dataset Collection:

The dataset used is the Power System Intrusion Detection dataset, which comprises 54 distinct features representing various attributes related to smart grid security and operations. It contains a total of 5 data entries, each detailing specific instances of power system behavior. These features capture critical information needed for detecting and preventing cybersecurity intrusions in intelligent electronic devices within smart grids.

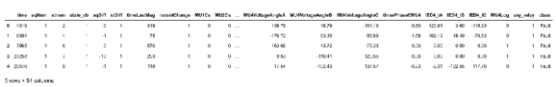


Fig.2 Dataset Collection Table

ii) Pre-Processing:

The preprocessing phase involves refining the dataset for optimal analysis by removing duplicate entries, cleaning unnecessary data, applying label encoding, visualizing key patterns, selecting significant features, and splitting the dataset into training and validation sets for effective model training.

a) Data Processing: Data processing ensures the dataset is clean and ready for analysis by performing crucial steps. Duplicate data entries are identified and removed to prevent redundancy, while irrelevant or noisy data is dropped to enhance the dataset's quality. These steps ensure consistency and reliability in the dataset, allowing for accurate insights during analysis and modeling. Proper data processing is essential for building effective machine learning models and achieving meaningful results.

b) Data Visualization: Data visualization involves creating graphical representations to better understand patterns, trends, and relationships within the dataset. It helps identify anomalies, correlations, and distributions of features, offering deeper insights into the data. Techniques such as bar charts, scatter plots, and heatmaps are utilized to interpret feature importance and class distributions. Visualization plays a vital role in preprocessing, enabling informed decisions for model building and improving the overall performance of machine learning algorithms.

c) Label Encoding: Label encoding converts categorical data into numerical format, making it suitable for machine learning models. Each unique category in a feature is assigned a distinct numeric value, ensuring that algorithms can process the data effectively. This technique is particularly useful for transforming non-numerical labels into a machine-readable form. By preserving the information in categorical features, label encoding enhances the model's ability to analyze patterns and make accurate predictions based on the encoded data.

d) Feature Selection: Feature selection involves identifying and retaining the most relevant attributes in the dataset while eliminating redundant or insignificant features. This process enhances model performance by reducing complexity, improving accuracy, and minimizing overfitting. Techniques such as correlation analysis, mutual information, or feature importance scores are commonly applied. By focusing on key features that contribute the most to predictions, feature selection optimizes computational efficiency and ensures the machine learning model achieves robust results.

iii) Training & Testing:

The dataset is divided into training and testing subsets to evaluate the machine learning model's performance effectively. The training set is used to teach the model patterns and relationships within the data, while the testing set assesses its ability to generalize to unseen instances. This split ensures reliable performance evaluation, reduces the risk of overfitting, and validates the model’s accuracy and efficiency in real-world scenarios.

iv) Algorithms:

SVM: Support Vector Machine (SVM) is a supervised machine learning algorithm used for classification and regression tasks. It constructs a hyperplane in a high-dimensional space that best separates data points of different classes. SVM is particularly effective in binary classification, where it aims to maximize the margin between two classes. In intrusion detection, SVM helps to classify data into normal or attack classes, making it suitable for cybersecurity applications in smart grids [9][10].

One Class-SVM: One-Class SVM is a variant of SVM used for anomaly detection. Unlike traditional SVM, which classifies data into multiple classes, One-Class SVM is trained on data from only one class and identifies data points that deviate significantly from the norm. It is ideal for detecting unknown threats or novel attacks in smart grids. One-Class SVM is widely employed for detecting outliers in cybersecurity datasets, where previously unseen or rare attacks are identified [9][10].

Gradient Boosting: Gradient Boosting is an ensemble learning algorithm that builds a model in a sequential manner, with each new model correcting the errors of the previous one. It focuses on improving predictive accuracy by optimizing a loss function iteratively. In cybersecurity, it is used for classification tasks, including detecting cyber-attacks in smart grids. Its ability to handle both binary and multi-class classification tasks makes it an effective tool for identifying complex threat patterns in intrusion detection systems [10][11].

LightGBM: LightGBM (Light Gradient Boosting Machine) is a fast, distributed, high-performance implementation of gradient boosting. It uses a histogram-based learning method that significantly speeds up training time while maintaining high accuracy. In the context of intrusion detection, LightGBM excels in classifying both binary and multi-class threats due to its ability to handle large datasets and complex feature interactions. It is particularly effective in identifying subtle attack patterns in smart grids, enhancing the overall system's cybersecurity defenses [10][11][12].

Stacking Classifier (Random Forest, LightGBM, and ExtraTreesClassifier): The Stacking Classifier combines multiple base models, such as Random Forest, LightGBM, and ExtraTreesClassifier, to make final predictions. Each model is trained on the dataset, and their outputs are combined to produce the most accurate prediction. The Stacking Classifier leverages the strengths of different algorithms to improve classification performance, particularly in complex tasks like intrusion detection in smart grids. This ensemble method excels in both binary and multi-class classification tasks, effectively identifying cyber threats and improving detection accuracy [8][10][12].

4. RESULTS & DISCUSSION

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:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

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:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)$$

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.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} \ + \ \mathrm{FN}} (3)$$

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.

$$F1\ Score = 2 * \frac{Recall\ \mathrm{X}\ Precision}{Recall + Precision} * 100 (1)$$

Table (1) evaluate the performance metrics — accuracy, precision, recall and F1-Score—for each algorithm. Across all metrics, the Stacking Classifier (RandomForest + LightGBM + ExtraTreesClassifier) consistently outperforms all other algorithms. The tables also offer a comparative analysis of the metrics for the other algorithms.

Table (2) evaluate the performance metrics — accuracy, precision, recall and F1-Score—for each algorithm. Across all metrics, the Stacking Classifier (RandomForest + LightGBM + ExtraTreesClassifier) consistently outperforms all other algorithms. The tables also offer a comparative analysis of the metrics for the other algorithms.

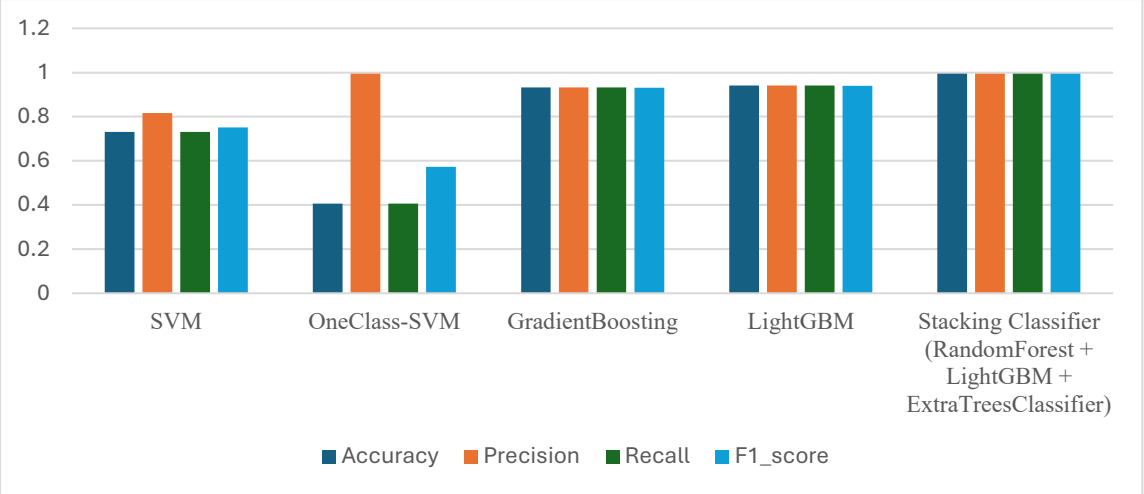
Table.1 Performance Evaluation Metrics for Binary class

ML Model	Accuracy	Precision	Recall	F1_score
SVM	0.731	0.816	0.731	0.751
OneClass-SVM	0.406	0.995	0.406	0.573
GradientBoosting	0.932	0.932	0.932	0.931
LightGBM	0.941	0.941	0.941	0.940
Stacking Classifier (RandomForest + LightGBM + ExtraTreesClassifier)	**0.995**	**0.995**	**0.995**	**0.995**

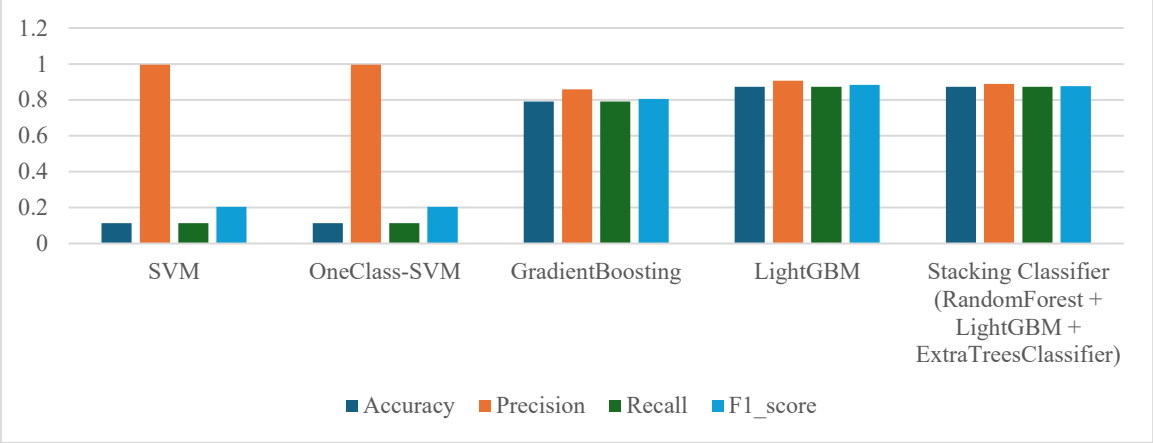
Table.2 Performance Evaluation Metrics for Multi class

ML Model	Accuracy	Precision	Recall	F1_score
SVM	0.114	0.995	0.114	0.205
OneClass-SVM	0.114	0.995	0.114	0.205
GradientBoosting	0.790	0.859	0.790	0.805
LightGBM	0.872	0.907	0.872	0.884
Stacking Classifier (RandomForest + LightGBM + ExtraTreesClassifier)	**0.872**	**0.889**	**0.872**	**0.877**

Graph.1 Comparison Graphs for Binary class



Graph.2 Comparison Graphs for Multi class



Accuracy is represented in light blue, precision in orange, recall in grey, and F1-Score in light yellow, ***Graph (1)***. In comparison to the other models, the Stacking Classifier (RandomForest + LightGBM + ExtraTreesClassifier) shows superior performance across all metrics, achieving the highest values. The graphs above visually illustrate these findings.

Accuracy is represented in light blue, precision in orange, recall in grey, and F1-Score in light yellow, ***Graph (2)***. In comparison to the other models, the Stacking Classifier (RandomForest + LightGBM + ExtraTreesClassifier) shows superior performance across all metrics, achieving the highest values. The graphs above visually illustrate these findings.

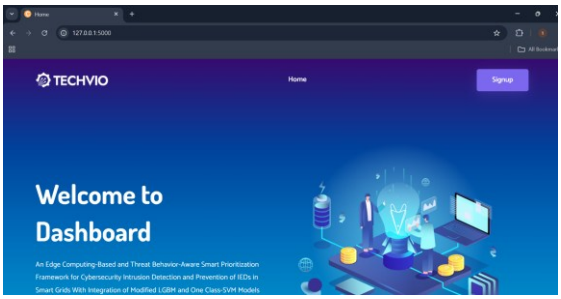


Fig. 3 Dash Board

The Fig. 3 shows the homepage of a cybersecurity platform called Techvio. It welcomes users to the dashboard and highlights its focus on edge computing, threat behavior analysis, and smart prioritization for intrusion detection.

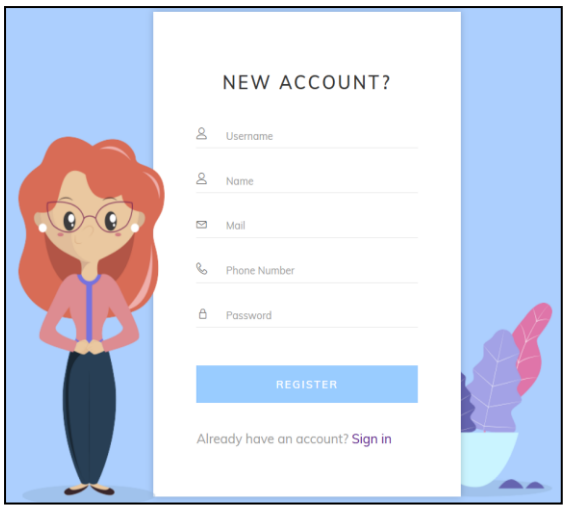


Fig. 4 Register Page

The Fig. 4 shows a user registration form with a cartoon woman illustration. It asks for a username, name, email, phone number, and password. There's a "REGISTER" button and a link to "Sign in" for existing users.

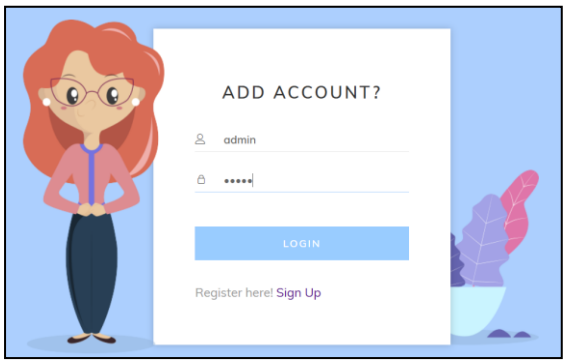


Fig. 5 Login page

The Fig. 5 shows a login page with a cartoon woman illustration. It has a pre-filled username "admin" and asks for a password. There's a "LOGIN" button and a link to "Sign Up" for new users.

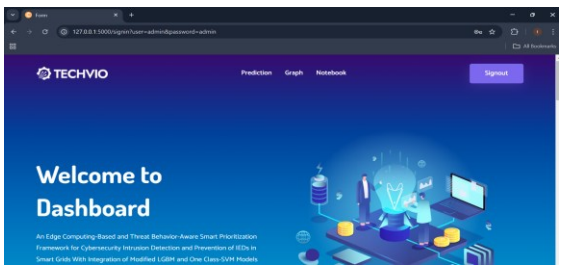


Fig. 6 Home page

The Fig. 6 shows the homepage of a cybersecurity platform called Techvio. It welcomes users to the dashboard and highlights its focus on edge computing, threat behavior analysis, and smart prioritization for intrusion detection.

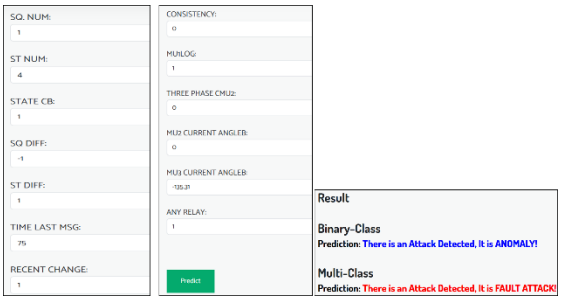


Fig. 7 Test case – 1

The Fig. 7 shows a network intrusion detection form. It collects data like sequence number, state, current angle, and other network statistics. After inputting data, the form predicts the outcome as an "Anomaly" and a "Fault Attack."

Step – 9
Test case 2

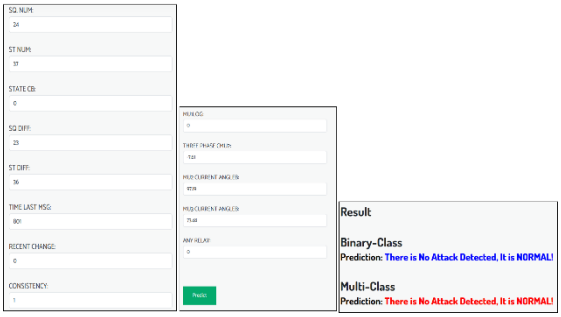


Fig. 7 Test case – 2

The Fig. 7 shows a network intrusion detection form. It collects data like sequence number, state, current angle, and other network statistics. After inputting data, the form predicts that "No Attack Detected, it is NORMAL!" for both binary-class and multi-class predictions.

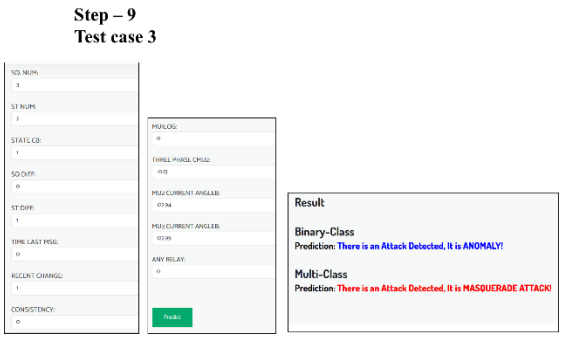


Fig. 7 Test case – 3

The Fig. 7 shows a network intrusion detection form. It collects data like sequence number, state, current angle, and other network statistics. After inputting data, the form predicts the outcome as an "Anomaly" and a "Masquerade Attack."

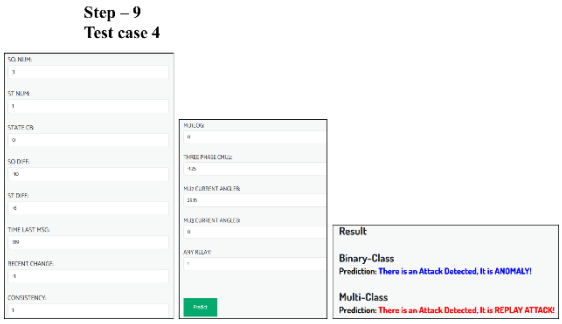


Fig. 7 Test case – 4

The Fig. 7 shows a network intrusion detection form. It collects data like sequence number, state, current angle, and other network statistics. After inputting data, the form predicts the outcome as an "Anomaly" and a "Replay Attack."

5. CONCLUSION

In conclusion, the proposed smart prioritization framework for intrusion detection and prevention in intelligent electronic devices (IEDs) within smart grids, leveraging edge computing, demonstrates significant performance improvements in cybersecurity. The integration of machine learning algorithms, including SVM, One-Class SVM, Gradient Boosting, LightGBM, Random Forest, and the Stacking Classifier, is crucial for detecting and mitigating complex cyber threats in real time. Among these, the Stacking Classifier, which combines Random Forest, LightGBM, and ExtraTreesClassifier, achieves the highest performance, showcasing its ability to handle both binary and multi-class classification tasks effectively. With an accuracy of 99.5% in binary classification and 87.2% in multi-class classification, the Stacking Classifier proves to be the most effective algorithm in identifying threat behaviors in the Power System Intrusion Detection dataset. This approach provides robust, reliable, and scalable intrusion detection for smart grid environments, enhancing cybersecurity by prioritizing critical alerts and enabling swift responses to potential threats. The results underline the system ' s potential in reinforcing security within the evolving landscape of smart grids.

Future improvements could focus on further enhancing the Stacking Classifier ' s performance by exploring additional ensemble methods or hybrid algorithms. Integrating real-time data streams and expanding the dataset to include diverse attack scenarios could improve generalization. Moreover, incorporating deep learning techniques, such as neural networks, may help detect more sophisticated threats. Continued development of the framework will strengthen smart grid cybersecurity, ensuring it adapts to emerging challenges and evolving attack vectors.

REFERENCES

[1] Chauhan, S. K., & Chauhan, V. S. (2024). Applications and Advancements in Energy Storage for Smart Grids. In Modeling, Analysis, and Control of Smart Energy Systems (pp. 17-41). IGI Global.

[2] Kiasari, M., Ghaffari, M., & Aly, H. H. (2024). A comprehensive review of the current status of smart grid technologies for renewable energies integration and future trends: the role of machine learning and energy storage systems. Energies, 17(16), 4128.

[3] Kavya, B. M., Mallikarjunaswamy, S., Sharmila, N., Shilpa, M., Komala, M., Shivaji, R., ... & Pavithra, G. S. (2024, August). An Efficient Machine Learning-Based Power Management System for Smart Grids Using Renewable Energy Resources. In 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON) (pp. 1-7). IEEE.

[4] Hatami, M., Nasab, M. A., Chen, Y., Mohammadi, J., Cruz, E. A., & Blasch, E. (2024, September). Optimizing Energy Storage Systems Deployment in Smart Grids. In 2024 IEEE ANDESCON (pp. 1-6). IEEE.

[5] Bhutta, M. S., Li, Y., Abubakar, M., Almasoudi, F. M., Alatawi, K. S. S., Altimania, M. R., & Al-Barashi, M. (2024). Optimizing solar power efficiency in smart grids using hybrid machine learning models for accurate energy generation prediction. Scientific Reports, 14(1), 17101.

[6] Roberts, E. (2024). AI-Driven Optimization of Energy Consumption in Smart Grids.

[7] Babanazarov, N. S., Matkarimov, A. I., & Ilyasov, I. S. (2024). Advancing energy efficiency: Harnessing machine learning for smart grid management. In E3S Web of Conferences (Vol. 524, p. 01003). EDP Sciences.

[8] Wang, J., Si, Y., Zhu, Y., Zhang, K., Yin, S., & Liu, B. (2024). Cyberattack detection for electricity theft in smart grids via stacking ensemble GRU optimization algorithm using federated learning framework. International Journal of Electrical Power & Energy Systems, 157, 109848.

[9] Li, X. J., Ma, M., & Sun, Y. (2023). An adaptive deep learning neural network model to enhance machine-learning-based classifiers for intrusion detection in smart grids. Algorithms, 16(6), 288.

[10] Yu, T., Da, K., Wang, Z., Ling, Y., Li, X., Bin, D., & Yang, C. (2022). An advanced accurate intrusion detection system for smart grid cybersecurity based on evolving machine learning. Frontiers in Energy Research, 10, 903370.

[11] Zhukabayeva, T., Pervez, A., Mardenov, Y., Othman, M., Karabayev, N., & Ahmad, Z. (2024). A traffic analysis and node categorizationaware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids. IEEE Access.

[12] Mhmood, A. A., Ergül, Ö., & Rahebi, J. (2024). Detection of cyber-attacks on smart grids using improved VGG19 deep neural network architecture and Aquila optimizer algorithm. Signal, Image and Video Processing, 18(2), 1477-1491.

[13] Zhao, H., Liu, G., Sun, H., Zhong, G., Pang, S., Qiao, S., & Lv, Z. (2023). An enhanced intrusion detection method for AIM of smart grid. Journal of Ambient Intelligence and Humanized Computing, 14(5), 4827-4839.

[14] Alani, M. M., Mauri, L., & Damiani, E. (2023). A two-stage cyber attack detection and classification system for smart grids. Internet of Things, 24, 100926.

[15] Panthi, M., & Das, T. K. (2022). Intelligent intrusion detection scheme for smart power-grid using optimized ensemble learning on selected features. International Journal of Critical Infrastructure Protection, 39, 100567.