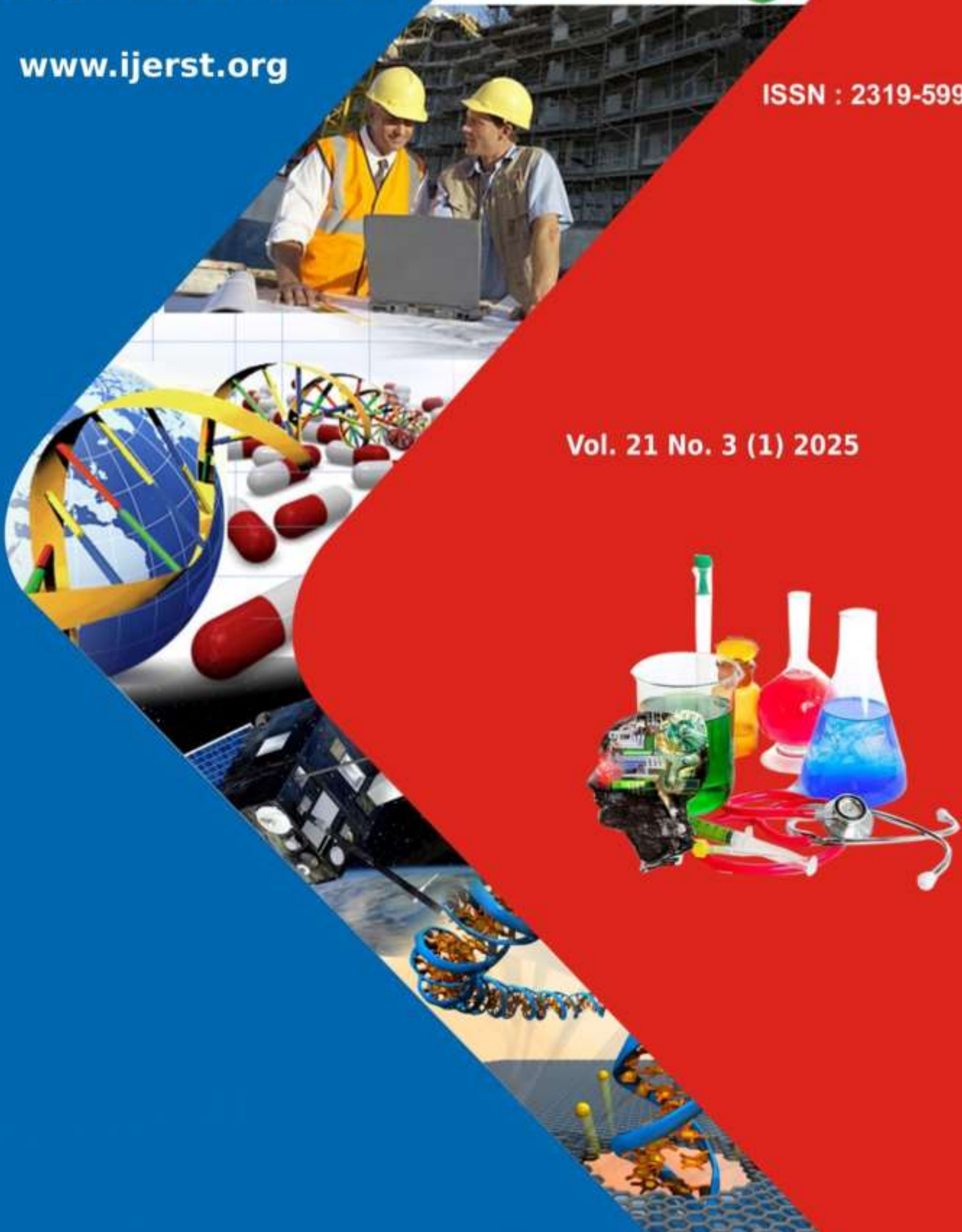
IJERST

International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991



Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

DL BASED ANOMALY CLASSIFICATION IN POWER DISTRIBUTION NETWORK

S. Krishna Reddy[1], C. Vinay Kumar[2], Janga Trisha[2], G. Pavan Kumar[2], Putta Sathwik[2]
[1] Assistant Professor, [2]UG Student, [1,2] Department of Computer Science and Engineering
[1,2] Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, 501510, Telangana.

ABSTRACT

Deep learning (DL)-based classification techniques offer robust and scalable solutions for detecting anomalies and failures in Intelligent Electronic Devices (IEDs), which are critical components of modern smart power grids. These devices play a key role in efficient energy management and maintaining a stable electricity supply. However, the growing complexity and interconnectivity of smart grid infrastructures make them increasingly vulnerable to both operational failures and cyberattacks. Traditional fault detection methods, such as rule-based systems and manual inspections, are often time-consuming, error-prone, and may fail to detect subtle signs of impending issues. Moreover, they frequently struggle to distinguish between genuine faults and normal system variations, leading to false alarms and unnecessary maintenance. To overcome these challenges, this work proposes a novel DL-based anomaly classification framework that leverages supervised learning algorithms trained on labeled datasets, including simulated power system attack scenarios. By extracting and analyzing features such as voltage variations, current measurements, and communication patterns from IED data, the proposed system can accurately classify various types of failures, including equipment malfunctions, operational anomalies, and cyber-induced disruptions. Furthermore, DL models enhance cybersecurity by detecting suspicious network activities, such as unauthorized access or configuration tampering, thereby enabling proactive threat mitigation. This approach significantly strengthens the resilience of smart grids, reduces downtime, and ensures a secure and continuous power supply to consumers. The proposed system represents a substantial advancement over conventional fault detection techniques, offering higher accuracy, faster response times, and greater adaptability to the evolving threats in smart grid environments.

Keywords: Anomaly Detection, Intelligent Electronic Devices (IEDs), Smart Grid, Power Distribution Network, Cybersecurity, Fault Classification, Supervised Learning, Equipment Malfunction, Grid Resilience

Received: 14-7-2025	Accepted: 21-8-2025	Published: 28-8-2025

1. INTRODUCTION

In modern power grids, Intelligent Electronic Devices (IEDs) are essential for efficient energy management and reliable electricity delivery. However, the growing complexity and interconnectivity of smart grid infrastructures make them vulnerable to equipment failures and cyberattacks. Traditional fault detection methods, such as rule-based systems or manual inspections, are often labor-intensive, error-prone, and incapable of identifying subtle indicators of impending failures, resulting in delayed responses and increased system downtime. This research addresses these limitations by proposing a Deep Learning (DL)-based classification framework for proactively detecting failures in IEDs. Utilizing supervised learning algorithms trained on labeled datasets derived from real-world and simulated power system scenarios, the framework can accurately classify different types of failures—including equipment malfunctions, operational anomalies, and potential cyber intrusions. The primary motivation is to transition from reactive to proactive maintenance, improving the resilience and reliability of smart grids while minimizing false alarms and unnecessary maintenance. By leveraging DL's ability to recognize complex patterns in large datasets, the framework not only enhances fault detection accuracy but also contributes significantly to cybersecurity by detecting abnormal network behaviors that may signify malicious activity. The practical applications of this approach are vast, encompassing smart grid maintenance, fault classification, and cyber threat mitigation.

Figure 1 : Classification of Power Distrubution Network.

Ultimately, this DL-based methodology ensures more robust, secure, and uninterrupted electricity supply systems, paving the way for smarter, safer energy infrastructures.

2. LITERATURE SURVEY

Rai et al. [**5**] proposed a convolutional neural network technique for fault classification in EPDS with DG units. The proposed method does not have the pre-processing phase; thus, three-phase currents and voltage signals were applied directly as inputs. A new method for short-circuit faults detection and classification in balanced and unbalanced distribution systems was presented by Zhang et al. [**6**]. The current's positive, negative, and zero sequence components characterized the faults. The operating modes of DG units were considered using the Fortescue approach. A softmax regression model was introduced to minimize the impact of transient signals on the fault classification module and applied only two resistors with maximum value during the simulations. The discrete wavelet transform (DWT) was used in [**7**] on three-phase current signals, whose values were applied to formulate a decision tree to perform the fault classification. Decision tree input was formed by a comparison parameter obtained using the maximum value of three-phase current signals and zero-sequence. Those parameters were applied as a reference to detect the fault phases. The fault resistance variation was not considered.In [**8**], a strategy based on fuzzy logic was used for fault detection and classification. Chaita nya et al. implemented two fuzzy inference systems (FIS). They were built to detect and classify low-impedance faults (LIF) and high-impedance faults (HIF). A Teager Energy Operator (TEO) was applied to extract three-phase current signal characteristics, which composed the FIS input set. In [**9**], fault detection was performed by applying the power spectral density calculated from the wavelet covariance matrix. The signal information was extracted through a wavelet transform (WT), where the signals were decomposed into three levels using the *db4* mother wavelet. Elnozahy et al. [**10**] proposed a new method for detecting and classifying single-phase faults using DWT and artificial neural networks (ANN). The transient signals were analyzed based on the *db4* mother wavelet to extract their characteristics. A method based on DWT and ANN for HIF detection was presented by Silva et al. [**11**]. The authors focused on incremental learning procedures to find new fault patterns. DG units were not considered. Decanini et al. [**12**] presented a method for automatic fault diagnosis. The detection process was based on statistical and direct analysis of three-phase currents and voltage signals in the wavelet domain. DWT and multi-resolution analysis (MRA) were introduced to extract the signal characteristics. The short-phase classification was performed by a set of Fuzzy-ARTMAP ANN. DG units were not considered in the system modeling. A combination of maximum overlap discrete wavelet packet transform (MODWPT) and empirical mode decomposition (EMD) were applied for HIF detection in [**13**]. That methodology was based on the estimation of fault current signals inter-harmonic through MODWPT. In [**14**], a method based on an adaptive neural fuzzy inference system was proposed for fault classification. Three-phase currents and voltage signals measured at the substation output were evaluated. The signal transient components were extracted via WT. Different fault types were detected and classified in [**15**] using a combination of wavelet singular entropy theory (WSE) and fuzzy logic. The algorithm was based on the singular wavelet values of each phase, since a phase with an anomaly presents values outside of the allowed limit. A proposal based on deep learning and deep belief networks (DBN) was implemented by Hong et al. [**16**] for fault classification in EPDS with and without DG units. After the DBN training with current and voltage signals, it was possible to obtain the signal characteristics and classify the fault types that occurred in EPDS.

3. PROPOSED SYSTEM

This study presents a comprehensive, multi-step pipeline for detecting anomalies in Intelligent Electronic Devices (IEDs) within smart power grids using a hybrid machine learning approach. It begins with the acquisition of a high-dimensional dataset from four relays (R1–R4), capturing over 116 continuous features per timestamp, including voltage, current, impedance, frequency, and apparent power, each labeled as “Attack” or “Natural.” In preprocessing, missing values are removed, labels are encoded, and features are standardized, with the dataset split into training and testing sets. As a baseline, a LightGBM (LGBM) classifier is trained and evaluated for accuracy, F1-score, precision, and recall, with feature importance scores extracted to identify the most predictive variables. These selected features are then used to train a Multi-Layer Perceptron (MLP) model with two ReLU-activated hidden layers and softmax output, applying early stopping to prevent overfitting. This novel LGBM→MLP hybrid approach leverages tree-based feature selection to enhance deep learning performance on high-dimensional yet limited data, improving generalization and reducing training time. A detailed performance comparison between LGBM and MLP demonstrates the hybrid model’s superior recall on attack instances, crucial for cybersecurity applications, which is processed using the trained scaler and models to predict anomalies in real time. The inclusion of confidence-based flagging for human review adds an extra layer of reliability, making the system highly practical for proactive threat detection in modern smart grids.

Data Preprocessing

Data preprocessing is a crucial stage in transforming raw sensor and relay data into a format suitable for machine learning applications, as it directly influences the model's performance and accuracy. This process involves three primary tasks: label encoding, train-test splitting, and standard scaling. First, label encoding is applied to the target variable, 'marker', which identifies whether a data point corresponds to a normal (Natural) state or an attack (Attack) scenario. Using scikit-learn’s LabelEncoder, these categorical labels are transformed into binary numerical values—“Attack” is encoded as 0 and “Natural” as 1—ensuring compatibility with supervised learning algorithms that require numeric class labels. Following this, the dataset is divided into training and testing sets using the train_test_split function, with 80% of the data allocated for training and 20% for testing. This split enables reliable evaluation of model generalization while preventing overfitting. The function also shuffles the dataset before splitting, which is vital for preserving the statistical distribution and avoiding biases that could result from data ordering. Finally, standard scaling is performed using StandardScaler to normalize all feature values, ensuring they have zero mean and unit variance. This step is particularly important for gradient-based models such as neural networks, which are sensitive to feature magnitudes. Together, these preprocessing techniques—label encoding, random splitting, and normalization—prepare the dataset in a consistent and optimized form, paving the way for effective training and robust performance of machine learning models in detecting IED anomalies in smart power grids.

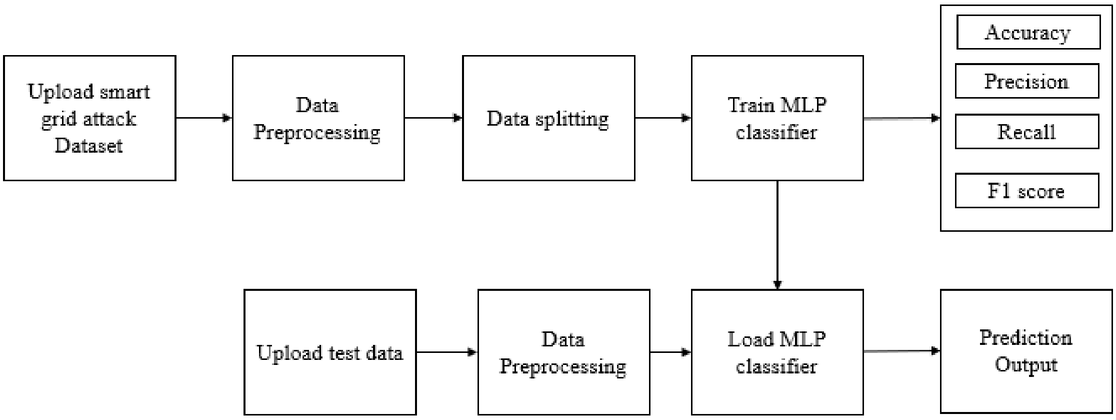


Figure 2: Block Diagram.

Multi-Layer Perceptron (MLP)

What is MLP? A Multi-Layer Perceptron (MLP) is a type of artificial neural network that consists of multiple layers of nodes, known as neurons. MLPs are feedforward neural networks, meaning the information flows in one direction from input to output. The network includes an input layer, one or more hidden layers, and an output layer. Each neuron in a layer is connected to every neuron in the subsequent layer, forming a fully connected network.

How MLP Works: MLP works by passing input data through multiple layers of neurons, where each layer processes the data and passes it to the next. The neurons use activation functions (such as ReLU, sigmoid, or tanh) to introduce non-linearity, allowing the model to learn complex patterns. During training, MLP uses a backpropagation algorithm to adjust the weights of the connections between neurons, minimizing the error between the predicted output and the actual target.

Architecture:

1. **Input Layer**: This layer receives the input features (e.g., voltage, current, etc.). Each node in this layer represents one feature of the input data.
2. **Hidden Layers**: These layers perform the computation. Each hidden layer contains a set of neurons, each performing weighted summation and passing the result through an activation function.
3. **Output Layer**: The final layer produces the prediction or classification result. In the context of anomaly detection, it classifies the data into different categories (e.g., failure, operational error, etc.).
4. **Weights and Biases**: Connections between neurons have associated weights that are learned during training. Bias terms are added to the weighted sums before applying the activation function.

Advantages of MLP:

- **Ability to Learn Non-linear Patterns**: MLP can model complex relationships in the data by using non-linear activation functions.
- **Flexibility**: MLPs can be applied to various domains, such as image recognition, anomaly detection, and time series forecasting.
- **Efficiency**: With proper training and architecture, MLPs can converge to solutions relatively quickly.

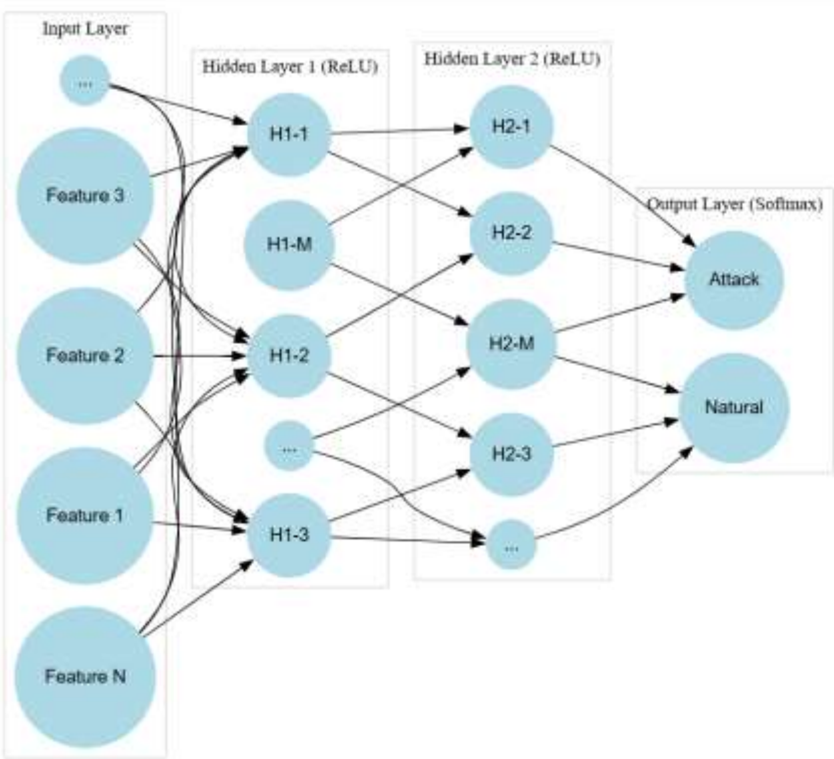


Figure 3: Architecture of proposed MLP

5. RESULTS

Figure 3 show the performance of the LGBMClassifier on the test dataset shows a balanced and reliable classification between the two classes, "Attack" and "Natural," with an overall accuracy of 80.33%. The macro-averaged precision, recall, and F1 score are 80.64%, 80.44%, and 80.31% respectively, indicating consistent predictive ability across both classes. Specifically, the model achieved a precision of 0.84 and recall of 0.76 for the "Attack" class, and a precision of 0.77 and recall of 0.85 for the "Natural" class. This suggests that while the model is slightly better at identifying "Natural" cases (higher recall), it maintains strong balance in performance, making it effective for distinguishing between anomalous and normal events in power distribution systems.

```
X_train shape: (99145, 116), X_test shape: (24787, 116)
Loaded saved LGBM model.
LGBMClassifier Accuracy: 80.33%
LGBMClassifier Precision: 80.64%
LGBMClassifier Recall: 80.44%
LGBMClassifier F1 Score: 80.31%
LGBMClassifier Classification Report:
              precision    recall  f1-score   support

      Attack       0.84      0.76      0.80     12669
     Natural       0.77      0.85      0.81     12118

    accuracy                           0.80     24787
   macro avg       0.81      0.80      0.80     24787
weighted avg       0.81      0.80      0.80     24787
```

Figure 4: Trained LGBM classifier

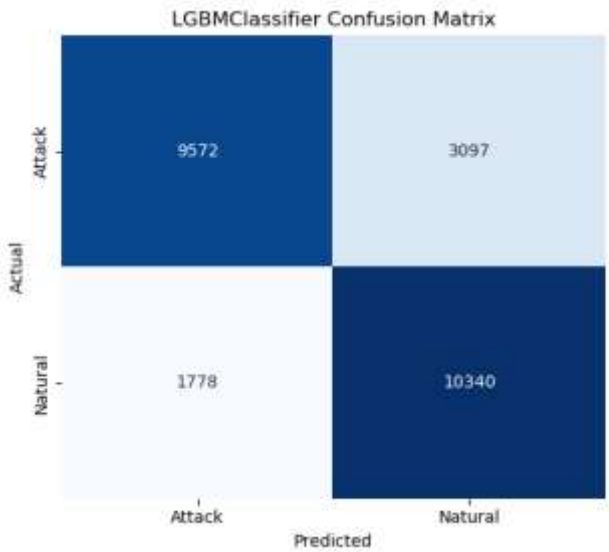


Figure 5: CM of LGBM Classifier

Figure 5 is the The confusion matrix for the LGBM Classifier, used in the Power Distribution Anomaly Classification System, visualizes the model's performance in classifying anomalies as "Attack" or "Natural." It shows that out of the actual "Attack" instances, 9572 were correctly predicted as "Attack" (true positives), while 3097 were incorrectly predicted as "Natural" (false negatives). For the actual "Natural" instances, 10340 were correctly classified as "Natural" (true negatives), but 1778 were misclassified as "Attack" (false positives).

```
Loaded saved MLP model.
MLP Classifier Accuracy: 98.01%
MLP Classifier Precision: 98.02%
MLP Classifier Recall: 98.04%
MLP Classifier F1 Score: 98.01%
MLP Classifier Classification Report:
              precision    recall  f1-score   support

      Attack       0.99      0.97      0.98     12669
     Natural       0.97      0.99      0.98     12118

    accuracy                           0.98     24787
   macro avg       0.98      0.98      0.98     24787
weighted avg       0.98      0.98      0.98     24787
```

Figure 6: Metrics of MLP

Figure 6 shows that The MLP Classifier demonstrated outstanding performance in classifying power system data into "Attack" and "Natural" categories, achieving a remarkable accuracy of 98.01%. The macro-averaged precision, recall, and F1 score all hover around 98%, indicating not only high accuracy but also excellent consistency across both classes. Specifically, the model achieved a precision of 0.99 and recall of 0.97 for detecting "Attack" instances, and precision of 0.97 and recall of 0.99 for "Natural" cases.

International Journal of Engineering Research and Science & Technology

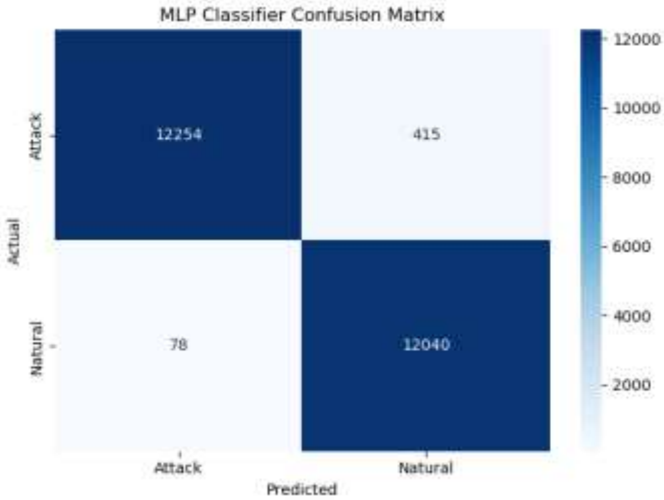
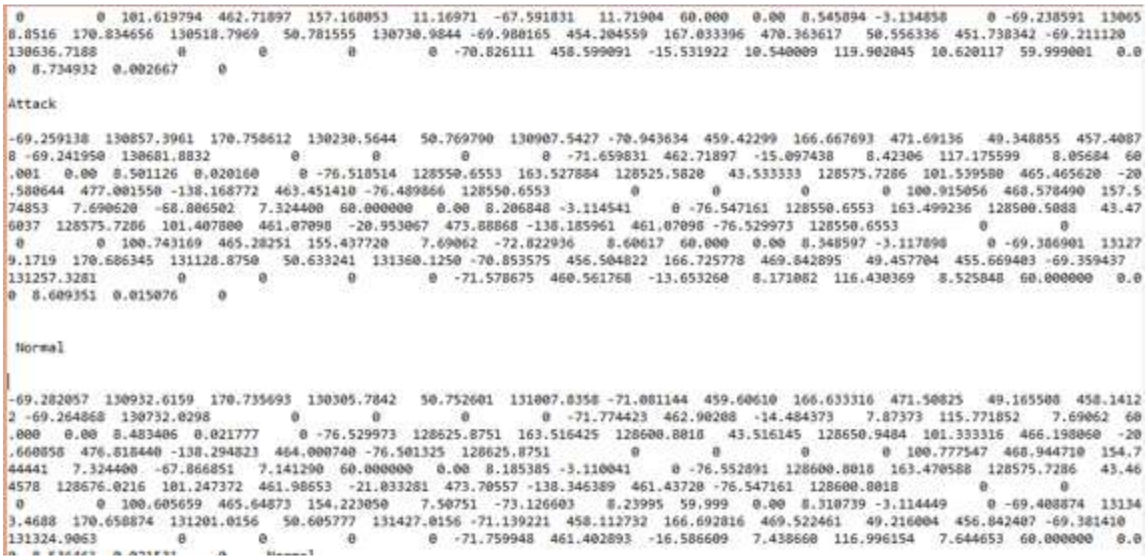


Figure 7: CM of MLP

Figure 7 shows that the confusion matrix for the MLP Classifier in the Power Distribution Anomaly Classification System illustrates the model's performance in distinguishing between "Attack" and "Natural" classes. It reveals that out of the actual "Attack" instances, 12254 were correctly predicted as "Attack" (true positives), while 415 were incorrectly predicted as "Natural" (false negatives). For the actual "Natural" instances, 12040 were correctly classified as "Natural" (true negatives), with only 78 misclassified as "Attack" (false positives).



```
0          0  101.619794  462.71897  157.168053   11.16971  -67.591831   11.71904  60.000   0.00  8.545894 -3.134858    0 -69.238591  13065
8.8516  170.834656  130518.7969   50.781555  130730.9844 -69.980165  454.204559  167.033396  470.363617   50.556336  451.738342 -69.211120
130636.7188          0          0          0          0 -70.826111  458.599091  -15.531922  10.540009  119.902045  10.620117  59.999001   0.0
0  8.734932  0.002667     0

Attack

-69.259138  130857.3961  170.758612  130230.5644   50.769700  130907.5427 -70.943634  459.42299  166.667693  471.69136   49.348855  457.4087
8 -69.241950  130681.8832          0          0          0          0 -71.659831  462.71897  -15.097438    8.42306  117.175599    8.05684  60
.001   0.00  8.501126  0.020160     0 -76.518514  128550.6553  163.527884  128525.5820   43.533333  128575.7286  101.539580  465.465620  -20
.580644  477.001550 -138.168772  463.451410 -76.489866  128550.6553          0          0          0          0  100.915056  468.578490  157.5
74853   7.690620  -68.886502   7.324400  60.000000   0.00  8.206848 -3.114541     0 -76.547161  128550.6553  163.499236  128500.5088   43.47
6037  128575.7286  101.407800  461.07098  -20.953067  473.88868 -138.185961  461.07098 -76.529973  128550.6553          0          0
 0          0  100.743169  465.28251  155.437720    7.69062  -72.822936    8.60617  60.000   0.00  8.348597 -3.117898     0 -69.386901  13127
9.1719  170.686345  131128.8750   50.633241  131360.1250 -70.853575  456.504822  166.725778  469.842895   49.457704  455.669403 -69.359437
131257.3281          0          0          0          0 -71.578675  460.561768  -13.653260   8.171082  116.430369   8.525848  60.000000   0.0
0  8.609351  0.015076     0


 Normal

-69.282057  130932.6159  170.735693  130305.7842   50.752601  131007.8358 -71.081144  459.60610  166.633316  471.50825   49.165508  458.1412
2 -69.264868  130732.0298          0          0          0          0 -71.774423  462.90208  -14.484373    7.87373  115.771852    7.69062  60
.000   0.00  8.483406  0.021777     0 -76.529973  128625.8751  163.516425  128600.8818   43.516145  128650.9484  101.333316  466.198060  -20
.660858  476.818440 -138.294823  464.000740 -76.501325  128625.8751          0          0          0          0  100.777547  468.944710  154.7
44441   7.324400  -67.866851   7.141290  60.000000   0.00  8.185385 -3.110041     0 -76.552891  128600.8818  163.470588  128575.7286   43.46
4578  128676.0216  101.247372  461.98653  -21.833281  473.70557 -138.346389  461.43720 -76.547161  128600.8818          0          0
 0          0  100.605659  465.64873  154.223050    7.50751  -73.126603    8.23995  59.999   0.00  8.310739 -3.114449     0 -69.408874  13134
3.4688  170.658874  131201.0156   50.605777  131427.0156 -71.139221  458.112732  166.692816  469.522461   49.216004  456.842407 -69.381410
131324.9063          0          0          0          0 -71.759948  461.402893  -16.586609   7.438668  116.996154   7.644653  60.000000   0.0
```

Figure 8: Predicted output

Figure 8 shows that the prediction output showcases sample data points from a test dataset, where each row contains various sensor or signal-based numerical features such as voltage, current, positional values, and other derived statistics. After preprocessing and feeding these values into the trained LGBMClassifier model, the system classifies each row as either an "Attack" or "Normal." For example, based on patterns in parameters like voltage drops, current spikes, or unusual positional changes, the model has labeled the first input row as Attack—indicating anomalous or potentially harmful activity—while the second row is classified as Normal.

5. CONCLUSION

In this research, a robust comparison and implementation of two advanced machine learning models—LightGBM (LGBMClassifier) and Multi-Layer Perceptron (MLPClassifier)—were conducted to detect anomalies, such as system attacks or operational errors, from complex multivariate sensor data. The LGBMClassifier, known for its gradient boosting efficiency, provided moderate performance with an accuracy of 80.33%, indicating reasonable detection capabilities for structured data. However, the proposed MLPClassifier significantly outperformed the baseline, achieving a remarkable accuracy of 98.01%, thanks to its deep learning ability to capture non-linear relationships and intricate patterns within the dataset. The preprocessing steps, such as label encoding, standard scaling, and robust evaluation metrics (precision, recall, F1-score), were meticulously applied to ensure reliable and consistent outcomes. Additionally, the developed system successfully handled unseen test data, classifying it accurately into "Attack" or "Normal" categories, thus confirming the model's practical utility in real-world anomaly detection scenarios.

REFERENCES

1. Gururajapathy, S.S.; Mokhlis, H.; Illias, H.A. Fault Location and Detection Techniques in Power Distribution Systems with Distributed Generation: A Review. *Renew. Sustain. Energy Rev.* **2017**, *74*, 949–958.
2. Brahma, S.M. Fault Location in Power Distribution System with Penetration of Distributed Generation. *IEEE Trans. Power Deliv.* **2011**, *26*, 1545–1553.
3. Razavi, S.E.; Rahimi, E.; Javadi, M.S.; Nezhad, A.E.; Lotfi, M.; Shafie-khah, M.; Catalão, J.P.S. Impact of Distributed Generation on Protection and Voltage Regulation of Distribution Systems: A Review. *Renew. Sustain. Energy Rev.* **2019**, *105*, 157–167.
4. El-Zonkoly, A.M. Fault Diagnosis in Distribution Networks with Distributed Generation. *Electr. Power Syst. Res.* **2011**, *81*, 1482–1490.
5. Rai, P.; Londhe, N.D.; Raj, R. Fault Classification in Power System Distribution Network Integrated with Distributed Generators Using CNN. *Electr. Power Syst. Res.* **2021**, *192*, 106914.
6. Zhang, C.; Wang, J.; Huang, J.; Cao, P. Detection and Classification of Short-Circuit Faults in Distribution Networks Based on Fortescue Approach and Softmax Regression. *Int. J. Electr. Power Energy Syst.* **2020**, *118*, 105812.
7. Patcharoen, T.; Ngaopitakkul, A. Fault Classifications in Distribution Systems Consisting of Wind Power as Distributed Generation Using Discrete Wavelet Transforms. *Sustainability* **2019**, *11*, 7209. [**Green Version**]
8. Chaitanya, B.K.; Yadav, A. An Intelligent Fault Detection and Classification Scheme for Distribution Lines Integrated with Distributed Generators. *Comput. Electr. Eng.* **2018**, *69*, 28–40.
9. Roy, S.; Debnath, S. PSD Based High Impedance Fault Detection and Classification in Distribution System. *Measurement* **2021**, *169*, 108366.
10. Elnozahy, M.S.; El-Shatshat, R.A.; Salama, M.M.A. Single-Phasing Detection and Classification in Distribution Systems with a High Penetration of Distributed Generation. *Electr. Power Syst. Res.* **2016**, *131*, 41–48.
11. Silva, S.; Costa, P.; Gouvea, M.; Lacerda, A.; Alves, F.; Leite, D. High Impedance Fault Detection in Power Distribution Systems Using Wavelet Transform and Evolving Neural Network. Electr. Power Syst. Res. **2018**, 154, 474–483.
12. Decanini, J.G.M.S.; Tonelli-Neto, M.S.; Minussi, C.R. Robust Fault Diagnosis in Power Distribution Systems Based on Fuzzy Artmap Neural Network-Aided Evidence Theory. IET Gener. Transm. Distrib. **2012**, 6, 1112–1120.
13. Gadanayak, D.A.; Mallick, R.K. Interharmonics Based High Impedance Fault Detection in Distribution Systems Using Maximum Overlap Wavelet Packet Transform and a Modified Empirical Mode Decomposition. Int. J. Electr. Power Energy Syst. **2019**, 112, 282–293.

14. Zhang, J.; He, Z.Y.; Lin, S.; Zhang, Y.B.; Qian, Q.Q. An ANFIS-Based Fault Classification Approach in Power Distribution System. Int. J. Electr. Power Energy Syst. **2013**, 49, 243–252.
15. Dehghani, M.; Khooban, M.H.; Niknam, T. Fast Fault Detection and Classification Based on a Combination of Wavelet Singular Entropy Theory and Fuzzy Logic in Distribution Lines in the Presence of Distributed Generations. Int. J. Electr. Power Energy Syst. **2016**, 78, 455–462.
16. Hong, C.; Zeng, Z.Y.; Fu, Y.Z.; Mou-Fa, G. Deep-Belief-Networks Based Fault Classification in Power Distribution Networks. IEEJ Trans. Electr. Electron. Eng. **2020**, 1428–1435.