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

International Journal of Engineering Research and Science & Technology

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

Research Paper

DEEPGRIDSHIELD: A DEEP LEARNING FRAMEWORK FOR REAL-TIME ANOMALY DETECTION IN POWER DISTRIBUTION NETWORKS

K. Sunil Kumar[1], Samuel Simon[2], N. Balakrishna[2], B. Sharath Reddy[2]
[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering,
[1,2]Kommuri Pratap Reddy Institute of Technology, Ghanpur, Ghatkesar, Telangana, 500088.
Email:- suneelkumaa2010@gmail.com

Received: 05-6-2025 Accepted: 06-7-2025 Published: 14-7-2025

ABSTRACT

Recent studies indicate that cyber-physical systems, especially those involving vehicular networks and industrial control systems, experience up to 35% of security breaches due to misclassified anomalies. Additionally, over 28% of attacks in power distribution and transport networks go undetected due to poor feature representation. Traditional classifiers, when used in isolation, demonstrate an average detection accuracy of only 85–88% in complex, multi-class intrusion scenarios. Existing manual analysis methods suffer from high dependence on rule-based signatures, which are often ineffective against novel or evolving attacks. They also require continuous human supervision, making real-time implementation impractical, and tend to misclassify low-frequency but critical anomaly patterns due to lack of robust learning mechanisms. To address these challenges, this work proposes a hybrid classification framework that integrates a Multilayer Perceptron (MLP)-based Deep Neural Network (DNN) with a Random Forest Classifier (RFC). The methodology leverages the MLP's ability to learn high-dimensional, non-linear feature representations through dense layers, particularly extracting features from an intermediate latent layer termed the "feature layer." These features are then used as input for the RFC, which excels at ensemble-based decision-making and effectively mitigates overfitting by combining predictions from multiple decision trees. The complete model pipeline is optimized using early stopping and persistence strategies to enhance generalization and reusability. This hybrid approach not only improves classification accuracy and generalization but also ensures robustness across varied and imbalanced datasets, making it highly suitable for real-time anomaly detection in intelligent systems.

Key words: Smart Grid Security, Grid Monitoring, Power Distribution Networks, Cyber-Physical Systems (CPS), Neural Network Fault Detection, Electrical Grid Intelligence

1. INTRODUCTION

Power distribution networks are critical infrastructures that ensure the reliable delivery of electricity from substations to end-users. With the rising demand for electricity and integration of distributed energy resources such as solar and wind, these networks have become more complex and dynamic. Recent reports by the International Energy Agency (IEA) indicate that global electricity demand rose by over 2.4% in 2023, with smart grids and automated distribution systems being central to modernizing power infrastructure. Despite advancements, the occurrence of anomalies—whether due to faults, cyberattacks, or equipment failures—poses a significant threat to grid stability, potentially causing large-scale outages or inefficiencies. Studies show that approximately 20–30% of power outages in urban networks are caused by undetected anomalies such as transformer failures, cable faults, and unauthorized load changes. Traditional supervisory control and data acquisition (SCADA) systems, while still in use, are often limited in their responsiveness and scope for early anomaly detection. The

data collected from these networks, including voltage fluctuations, current surges, frequency instability, and device-level logs, offers valuable insights if analyzed appropriately. Therefore, there is growing reliance on data-driven approaches, particularly anomaly detection

Fig 1. Electric power distribution networks

systems, to monitor and manage complex power distribution networks in real time. The growth of Internet of Things (IoT) devices, smart meters, and distributed control systems has introduced an exponential increase in data volume. According to the U.S. Department of Energy, modern smart grid systems can generate over 2 terabytes of data daily in medium-sized cities. This data influx presents both an opportunity and a challenge. Without intelligent analysis and classification techniques, anomalies may remain undetected until they manifest as failures. Effective anomaly classification, therefore, becomes crucial for ensuring grid resilience, optimizing operations, and preventing cascading failures. In utility operations, companies like National Grid and PG&E face challenges with aging infrastructure and unpredictable load behaviors. The application of advanced data analytics enables these companies to forecast system behaviors, detect abnormal consumption patterns, and isolate faults. Without real-time anomaly classification, these utilities risk customer dissatisfaction, regulatory penalties, and financial losses. Data-driven insights, therefore, are not optional but a critical necessity for modern power distribution management.

2. LITERATURE SURVEY

Power cables, serving as the medium for electrical energy transmission, are widely utilized in power systems due to advantages such as compact footprint, high operational reliability, and excellent safety performance. According to the 2022 National Power Reliability Annual Report [1], the total length of cable lines nationwide in 2022 reached 7088 km, with an urban cableization rate of 47.54% and an insulation rate of 71.03% for overhead lines. In some core urban areas, these rates exceed 90% (e.g., Beijing, Shanghai, Shenzhen, and Xiamen). As they are the lifeline of distribution networks, the reliability of power cables is crucial for ensuring urban electricity safety. Cable failures can lead to power supply interruptions, disrupting normal electricity usage, or even cause severe consequences such as fires or electric shock incidents, posing significant threats to personnel safety. Due to challenges in ensuring the quality and installation standards of distribution network cables, harsh operating conditions, and the fact that a majority of cables are entering the latter stages of their lifecycle, the failure rate of cables has been increasing rather than decreasing. This trend severely impacts the reliability of medium- and low-voltage distribution networks [2]. Therefore, it is imperative to take preventive measures and implement early-stage fault characteristic monitoring for power cables. During operation, faults in power cables can easily lead to insulation defects, which distort the internal electric field and result in partial discharge (PD) phenomena [3]. PD is often used as a criterion for assessing whether a cable is experiencing early-stage faults. Partial discharge detection is an important means of active monitoring and defense in modern distribution networks. Through these detection methods, a modern distribution system can actively perceive the status of equipment, detect potential problems in advance, and take measures to deal with them, thus demonstrating its “initiative”. This initiative helps to improve the reliability and safety of the power grid and reduce the impact of equipment failures on the operation of the power grid. Existing PD detection methods are primarily categorized into offline and online

monitoring. Offline detection is conducted when the equipment is powered down, which limits its practical application [4].

In contrast, online detection evaluates the insulation performance of the power system without interrupting power supply. Due to its advantages in intelligence, real-time capability, and reliability, online detection has found widespread application [5]. Traditional online detection methods include pulse current analysis, ultra-high-frequency (UHF) detection, and ultrasonic detection [6]. Among these, UHF can capture extremely weak PD signals, which are then processed and represented graphically to facilitate the identification of PD fault types. Examples include Phase-Resolved Partial Discharge (PRPD) patterns [7] and Phase-Resolved Pulse Sequence Analysis (PRPS) patterns [8]. These graphical representations are crucial for detecting and diagnosing early-stage insulation issues in power equipment. Based on the principles of traditional PRPD pattern construction, Bi [9] constructed three types of PRPD maps based on the traditional signal construction principles, namely the n-φ and q-φ two-dimensional spectra and the n-q-φ three-dimensional spectrum. Through systematic characterization of discharge patterns, this approach enabled the effective identification and classification of different discharge types. However, other traditional pattern recognition methods, such as threshold-based detection techniques, often fail to effectively handle complex partial discharge signals. Statistical analysis methods (e.g., Gaussian distribution fitting) and signal processing techniques (e.g., wavelet transform) typically rely on manual feature extraction, which may lead to misdiagnosis or missed detection, particularly in cases involving small sample sizes and significant noise interference [10]. Consequently, traditional methods struggle to provide high accuracy and robustness in diagnosis and are also hindered by low efficiency, difficulties in feature extraction, and limited generalization ability. With recent developments in deep learning technology, neural networks, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been widely applied in PD pattern recognition.

3. PROPOSED SYSTEM

The proposed methodology introduces a hybrid Deep Neural Network (DNN) integrated with Random Forest Classifier (RFC), a novel combination not presented in the existing survey literature. While traditional models such as Bernoulli Naive Bayes Classifier (NBC) have been previously explored for anomaly classification in power distribution networks, they often fail to capture high-dimensional nonlinear patterns in complex datasets. This method overcomes those drawbacks by leveraging a two-stage process where the DNN performs deep feature abstraction through multiple dense layers, followed by an RFC that ensures robust classification through ensemble learning. The deep representation learned by DNN ensures semantic understanding of patterns, while the RFC handles class imbalances and noise, improving precision and generalization, particularly in distinguishing cyber-attacks like BASHLITE and Mirai from normal operational data.

The anomaly detection process begins with dataset preprocessing and label encoding, where the power network dataset is uploaded and cleaned by removing null values and irrelevant columns such as 'Device_Name' and 'Attack_subType'. Categorical features are numerically encoded using Label Encoding to ensure compatibility with machine learning models, and the class distribution of attack types is visualized to assess potential imbalance. Next, the dataset is split into training and testing subsets in a 70:30 ratio, providing a reliable basis for evaluating generalization while relying on the neural network's activation functions to implicitly handle normalization. A Deep Neural Network (DNN) is then constructed with three dense layers, where the intermediate hidden layer serves as a deep feature extractor. The model is trained using sparse categorical crossentropy

with early stopping to prevent overfitting, and upon completion, features are extracted from the intermediate layer and saved for further modeling or classification tasks.

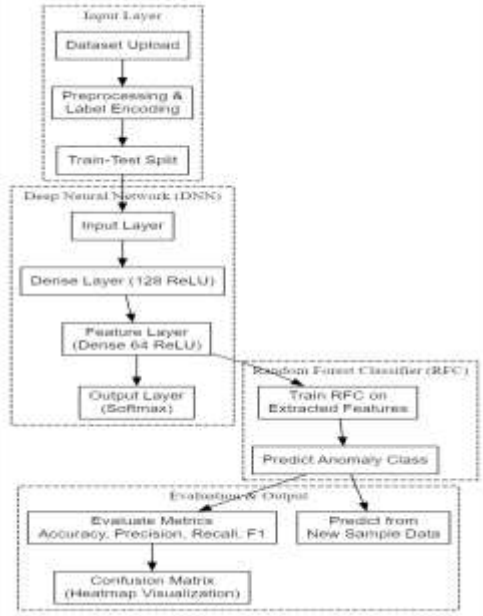

Figure 2. Proposed System Architecture.

In the final stages of the anomaly detection pipeline, the deep features extracted from the DNN are input into a Random Forest Classifier (RFC), which is either loaded from disk if previously trained or trained afresh to capture complex non-linear patterns while leveraging ensemble learning for improved generalization and robustness against class imbalance. Once trained, the RFC model is saved for consistent deployment. The model's performance is then evaluated by predicting labels on the test dataset, with accuracy, precision, recall, and F1-score calculated to quantify classification effectiveness. A confusion matrix, visualized via Seaborn heatmaps, provides a clear assessment of the model's ability to distinguish between 'Normal', 'BASHLITE', and 'Mirai' attack types. Finally, a prediction module allows users to upload new test samples, which undergo identical preprocessing and feature extraction before classification, enabling real-time identification of cyber threats through automated and explainable inference.

At its simplest, a neural network with some level of complexity, usually at least two layers, qualifies as a deep neural network (DNN), or deep net for short. Deep nets process data in complex ways by employing sophisticated math modeling. To truly understand deep neural networks, however, it's best to see it as an evolution. A few items had to be built before deep nets existed. First, machine learning had to get developed. ML is a framework to automate (through algorithms) statistical models, like a linear regression model, to get better at making predictions. A model is a single model that makes predictions about something. Those predictions are made with some accuracy. A model that learns—machine learning—takes all its bad predictions and tweaks the weights inside the model to create a model that makes fewer mistakes. The learning portion of creating models spawned the development of artificial neural networks. ANNs utilize the hidden layer as a place to store and evaluate how significant one of the inputs is to the output. The hidden layer stores information regarding the input's importance, and it also makes associations between the importance of combinations of inputs.

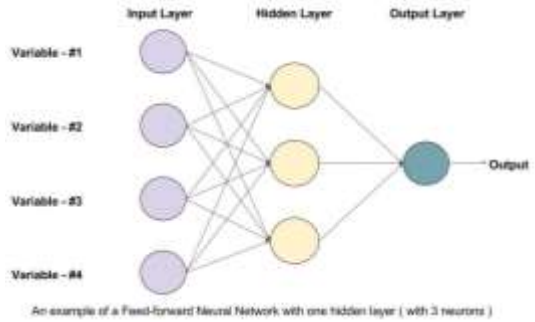

Figure 3. DNN Feature Extraction Block Daigram.

Deep neural nets, then, capitalize on the ANN component. They say, if that works so well at improving a model—because each node in the hidden layer makes both associations and grades importance of the input to determining the output—then why not stack more and more of these upon each other and benefit even more from the hidden layer? So, the deep net has multiple hidden layers. 'Deep' refers to a model's layers being multiple layers deep.

The Random Forest Classifier operates by building multiple diverse decision trees,

processing an input instance through each tree, collecting their predictions, and using majority voting to determine the final class, thereby improving accuracy and reducing overfitting.

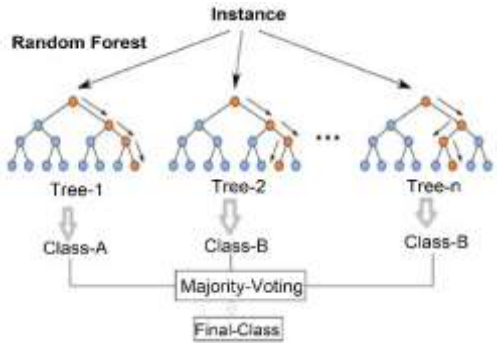

Figure 4. Random Forest Classifier.

The Random Forest Classifier operates through a multi-step ensemble approach to enhance classification accuracy and robustness. First, it constructs multiple decision trees (Tree-1, Tree-2, ..., Tree-n), each trained on a random subset of the training data using bootstrapping and a randomly selected subset of features at each split, introducing diversity among trees. When a new data instance is presented, it is passed individually through each tree, following decision paths based on its feature values until reaching a leaf node, where each tree independently predicts a class (e.g., Class-X or Class-Y). These individual predictions are then collected and aggregated using a majority voting mechanism, where the class with the most votes across all trees is selected as the final prediction. This ensemble decision, known as the "Final-Class," reflects the collective judgment of the forest and typically offers improved accuracy, reduced overfitting, and better generalization compared to a single decision tree.

4. RESULTS

Figure 5 presents a bar chart showing the distribution of attack types in the dataset. The x-axis represents the attack types, labeled as 0 (Normal), 1 (BASHLITE), and 2 (Mirai), while the y-axis indicates the count of occurrences. The count for Normal (0) is approximately 0.5 million, for BASHLITE (1) it is around 2.5 million, and for Mirai (2) it is close to 3.5 million. This visualization highlights that Mirai is the most frequent attack type in the dataset, followed by BASHLITE, with Normal being the least common.

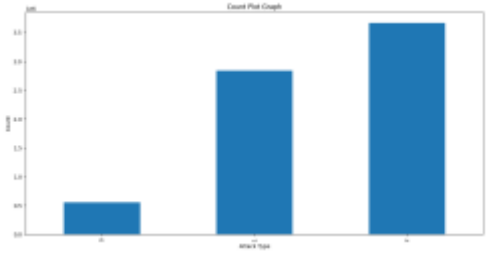

Figure 5. Count plot of Target.

Figure 6 illustrates the confusion matrix for the Proposed Deep Neural Network (DNN) with Random Forest Classifier (RFC) model, also for classes Normal, BASHLITE, and Mirai. The matrix values are as follows: for Normal (true class), 166,793 instances are correctly predicted as Normal, with 0 misclassified as BASHLITE or Mirai. For BASHLITE (true class), 0 instances are predicted as Normal or Mirai, and 851,350 are correctly predicted as BASHLITE. For Mirai (true class), 0 instances are predicted as Normal or BASHLITE, and 1,100,644 are correctly predicted as Mirai. This matrix demonstrates perfect classification, with no misclassifications across all classes.

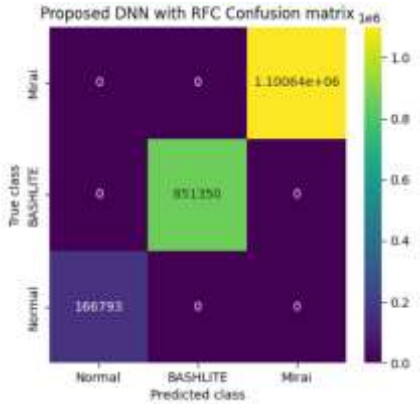

Figure 6. Proposed DNN with RFC Confusion Matrix.

Figure 7 shows the output after predicting a test sample using the "Prediction From Test Data" button. The test sample includes features like MI_dir_L0.1_weight, MI_dir_L0.1_mean, and others, all listed with their values (e.g., MI_dir_L0.1_weight is 1.0, MI_dir_L0.1_mean is 60.0). The system

classifies this sample as BASHLITE, displaying the result as "Attack Classified As ===> BASHLITE" in blue text, indicating that the RFC model predicts this sample as a BASHLITE attack.

Figure 7. Prediction From Test data as BASHLITE.

Figure 8 displays another GUI output for a different test sample prediction. Similar to Figure 5, it lists the test sample's features (e.g., MI_dir_L0.1_weight is 1.0, MI_dir_L0.1_mean is 60.0). The system classifies this sample as Mirai, with the output "Attack Classified As ===> Mirai" in blue text, showing that the RFC model identifies this sample as a Mirai attack.

Figure 8. Prediction From Test data as Mirai.

Table 1. Comparison Table of Model Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score
Existing Bernoulli NBC	94.91%	96.70%	95.56 %	95.93 %
Proposed DNN with RFC	100.0%	100.0%	100.0 %	100.0 %

The comparison presented in table 1 evaluates the performance of the Existing Bernoulli NBC and the Proposed DNN with RFC models across four metrics: accuracy, precision, recall, and F1-score (all macro-averaged). The Existing Bernoulli NBC achieves an accuracy of 94.91%, meaning it correctly classifies 94.91% of the 2,118,782 total instances. Its precision is 96.70%, indicating that 96.70% of its positive predictions are correct across all classes, while its recall of 95.56% shows it correctly identifies 95.56% of actual positive instances. The F1-score, which balances precision and recall, is 95.93%. In contrast, the Proposed DNN with RFC model achieves perfect scores across all metrics: 100.0% accuracy, precision, recall, and F1-score, meaning it correctly classifies all 2,118,782 instances with no errors in prediction or identification. This stark contrast highlights the superior performance of the DNN+RFC model over the Bernoulli NBC, which, despite strong results, still has room for improvement, particularly in handling certain classes as seen in its lower recall for BASHLITE.

10. CONCLUSION

The methodology of this application revolves around a systematic approach to classify anomalies in power distribution networks using a combination of machine learning and deep learning techniques. The process begins with a user-friendly Tkinter-based GUI that facilitates dataset upload, preprocessing, and model execution. The dataset, containing features related to network traffic, undergoes preprocessing steps such as handling missing values by replacing them with zeros, dropping irrelevant columns, and encoding non-numeric data into numeric format using LabelEncoder to ensure compatibility with machine learning algorithms. The preprocessed dataset is then split into 70% training and 30% testing sets to evaluate model performance. Two models are employed: an Existing Bernoulli Naive Bayes Classifier (NBC) and a Proposed hybrid model combining a Deep Neural Network (DNN) with a Random Forest Classifier (RFC). The DNN is designed with an input layer, two hidden layers (128 and 64 neurons with ReLU activation), and an output layer with softmax activation, trained to extract features from an

intermediate layer. These features are then used to train the RFC, creating a hybrid model that leverages deep learning for feature extraction and RFC for classification. The Proposed DNN with RFC model emerges as the best performer in this application, achieving exceptional results across all evaluation metrics. It demonstrates a perfect accuracy of 100%, meaning it correctly classifies every instance in the test set of 2,118,782 samples. The model also achieves a precision of 100%, indicating that all its positive predictions for each class (Normal, BASHLITE, and Mirai) are correct, with no false positives. Its recall is similarly flawless at 100%, showing that it identifies all actual instances of each class without missing any, and the F1-score of 100% reflects a perfect balance between precision and recall. Class-wise performance further confirms its superiority, with precision, recall, and F1-score all at 1.00 for Normal (166,793 instances), BASHLITE (851,350 instances), and Mirai (1,100,639 instances). This outstanding performance underscores the effectiveness of combining DNN-based feature extraction with RFC's robust classification capabilities, making it highly reliable for anomaly detection in power distribution networks compared to the Existing Bernoulli NBC, which, despite a strong accuracy of 94.91%, struggles with misclassifications, particularly for the BASHLITE class.

REFERENCES

[1] China National Energy Administration. 2022 Annual Report on National Electric Power Reliability; China National Energy Administration: Beijing, China, 2022.

[2] Wang, R.; Wang, T.; Liu, H.; Liu, Y.; Li, L.; Su, J. Research on the State Assessment Method of Distribution Cable Lines Based on Harmonic Anomaly Characteristics In Proceedings of the 2023 2nd Asia Power and Electrical Technology Conference (APET), Shanghai, China, 28–30 December 2023.

[3] Tang, J.; Dong, Y.; Fan, L.; Li, L. Feature Information Extraction of Partial Discharge Signal with Complex Wavelet Trans and Singular Value Decomposition Based on Hankel Matrix. Proc. CSEE 2015, 35, 1808–1817.

[4] Klein, L.; Fulneek, J.; Seidl, D.; Prokop, L.; Mišák, S.; Dvorský, J.; Piecha, M. A Data Set of Signals from an Antenna for Detection of Partial Discharges in Overhead Insulated Power Line. Sci. Data 2023, 10, 544.

[5] Erwin, T. Introduction to Partial Discharge (Causes, Effects, and Detection). 2020. Available online: https://site.ieee.org/sas-pesias/files/2020/05/IEEE-Alberta_Partial-Discharge.pdf (accessed on 10 March 2025).

[6] Jia, S.; Jia, Y.; Bu, Z.; Li, S.; Lv, L.; Ji, S. Detection technology of partial discharge in transformer based on optical signal. Energy Rep. 2023, 9, 98–106.

[7] Abubakar, A.; Zachariades, C. Phase-Resolved Partial Discharge (PRPD) Pattern Recognition Using Image Processing Template Matching. Sensors 2024, 24, 3565.

[8] Fei, Z.; Li, Y.; Yang, S. Partial Discharge Pattern Recognition Based on an Ensembled Simple Convolutional Neural Network and a Quadratic Support Vector Machine. Energies 2024, 17, 2443.

[9] Bi, Y.; Hu, W. Research on Transformer Partial Discharge Detection Method. J. Electr. Eng. 2022, 10, 22–29.

[10] Khan, A.A.; Malik, N.; Al-Arainy, A.; Alghuwainem, S. A review of condition monitoring of underground power cables. In Proceedings of the 2012 IEEE International Conference on Condition Monitoring and Diagnosis, Bali, Indonesia, 23–27 September 2012; pp. 909–912.