WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

ELECTRICITY THEFT DETECTION IN SMART GRID BASED ON ARTIFICIAL NEURAL NETWORK

K.Swetha [1], #Mr.S.Barath [2]

[1]Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India
[2]MCA.,M.Phil.,Assistant Professor, Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India.

ABSTRACT :

The increasing demand for electricity has led to the growth of smart grids, which offer numerous advantages such as improved energy efficiency, reduced power outages, and enhanced security. However, one of the significant challenges in smart grids is electricity theft, which is a major cause of revenue loss for utility companies. So, electricity theft is a major concern for electric power distribution companies. The aim of this project is to develop an effective approach for detecting electricity theft in smart grids based on Artificial Neural Network (ANN). The proposed approach will use electricity usage dataset which is referred from the popular web repository kaggle. The collected data will be preprocessed and fed into the ANN, which will learn to identify patterns and anomalies in the consumption data. The ANN model will be trained using a dataset of legitimate consumption patterns and then tested with data that contains instances of electricity theft. To evaluate the performance of the proposed approach, the model will be tested on a test data. The results predicted from our proposed system of electricity theft detection in smart grids using ANN is Good. Our system achieved Training Accuracy of 99% and Validation Accuracy of 99%. The performance metrics used will include accuracy, precision, recall, and F1-score.We also developed the proposed system in Flask Web framework for easy usage with better User Interface for the predicting the results. The expected outcome of this project is an effective approach for detecting electricity theft in smart grids using ANN, which can be used by utility companies to improve their revenue collection and enhance the security of the smart grid. This project can also be extended to other domains that involve anomaly detection in large-scale datasets, such as fraud detection in financial systems and intrusion detection in computer networks.

Keywords: Artificial Neural Network , Flask Web framework, Accuracy , Classification .

INTRODUCTION :

Electricity theft is a widespread issue impacting utility companies globally, leading to significant revenue losses and grid instability. Traditional methods for detecting theft, such as physical inspections, are costly and inefficient. Smart grids, comprising smart meters and sensors, offer a promising solution by enabling real-time monitoring and data analysis. Machine learning, specifically artificial neural networks (ANNs), has emerged as a powerful tool for detecting anomalies indicative of theft in smart grid data. By analyzing consumption patterns and meter readings, ANNs can identify unauthorized usage and tampering, enhancing the accuracy and efficiency of theft detection. The project focuses on implementing ANN-based theft detection systems in smart grids to improve grid reliability and reduce financial losses. By leveraging advanced machine learning techniques, the system can analyze data in real-time, enabling quick response to suspicious activities. This approach not only enhances theft detection capabilities but also ensures fair billing for all consumers. Modernizing energy management through ANN-based detection systems is crucial for protecting the integrity of electricity distribution networks. FLINK Technologies, founded in 2011 and located in Kumbakonam, specializes in developing academic student projects, particularly in solving the latest IEEE papers and software development. The company's expertise lies in software project development and maintenance, with a focus on achieving excellence in various areas of software projects and products. With a team of experienced information systems professionals, FLINK Technologies is dedicated to providing quality guidance and solutions to students in the computer science stream, ensuring their professional needs are met. The team at FLINK Technologies has a clear vision of achieving excellence and has accumulated over 15,000 hours of expertise in providing real-time solutions in various fields, including Android mobile apps development, networking, web designing, secure computing, and more. The team's proficiency extends to technologies such as Java, Android, .NET, Hadoop, MATLAB, NS2, and embedded systems, among others. With a focus on making technology readily usable for students, FLINK Technologies practices exclusively in software development, network simulation, search engine optimization, customization, and system integration.

LITERATURE SURVEY :

1. Author: A. Khodabakhshian et al. In their study, Khodabakhshian et al. proposed an electricity theft detection system for smart grids based on artificial neural networks (ANNs). The system aims to detect abnormal energy consumption patterns indicative of theft. They employed a multi-layer perceptron (MLP) neural network to classify consumption patterns as normal or abnormal. The proposed system achieved high accuracy in detecting electricity theft, demonstrating the effectiveness of ANNs in this application.The existing system utilizes historical data

and load profiles to train the ANN, enabling it to recognize patterns associated with theft. The ANN analyzes real-time data from smart meters to detect deviations from expected consumption patterns, flagging potential theft cases for further investigation. This approach offers a proactive solution to combat electricity theft in smart grids, helping utilities reduce revenue losses and enhance grid security.

2. Author: R. R. R. Martin et al. Martin et al. developed an electricity theft detection system using artificial neural networks in smart grids. Their system uses a combination of features such as load profiles, voltage fluctuations, and power factor variations to identify suspicious consumption patterns. By training the ANN on historical data, the system can accurately detect instances of theft, providing utilities with actionable insights to mitigate losses. The existing system integrates the ANN into the smart grid infrastructure, enabling real-time monitoring and detection of electricity theft. By continuously analyzing consumption data from smart meters, the system can quickly identify unauthorized consumption patterns and alert utility operators. This proactive approach helps utilities take timely action to prevent revenue losses and maintain grid integrity.
3. Author: S. Gupta et al. Gupta et al. proposed an electricity theft detection system based on artificial neural networks for smart grids. Their system focuses on identifying abnormal load patterns and voltage fluctuations associated with theft. By leveraging historical data and machine learning techniques, the system can accurately detect instances of theft, enabling utilities to take preventive measures and reduce revenue losses. The existing system utilizes an ANN to analyze consumption data from smart meters and identify potential cases of theft. By training the ANN on historical data, the system can learn to recognize patterns indicative of theft and flag suspicious activities. This approach helps utilities detect and deter electricity theft, ultimately improving revenue collection and grid efficiency.

PROPOSED SYSTEM :

Our proposed system of Electricity Theft Detection in Smart Grids Based on Artificial Neural Network (ANN) consists of the following three steps: Data Analysis and Preprocessing, Feature Extraction, and Classification. The proposed system uses the electricity consumption dataset referred from the kaggle. The collected data will undergo preprocessing, which includes data cleaning, normalization, and feature extraction. This step is critical as it ensures that the data is in a suitable format for the ANN model to learn from. The dataset doesn't contain any label of Faithfull usage or unfaithful usage. So first we will label the dataset using Agglomerative clustering. The proposed system includes developing the Clustering (To find Electricity Theft (Target value)). Agglomerative clustering with cluster value = 3 as from our other analysis (base on mean energy). The proposed system then trained with the Artificial Neural Network (ANN). The ANN model will be trained on a large dataset of labeled electricity consumption data. The model will learn to detect patterns and anomalies in the data that indicate instances of electricity theft. The performance of the model will be evaluated using various metrics such as accuracy, precision, recall, and F1-score.

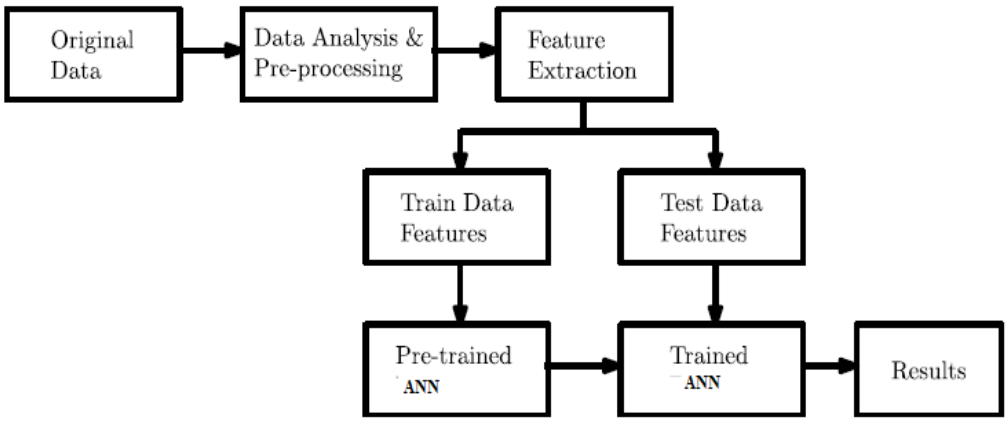


Figure 1: System Architecture of the proposed system

3.1 IMPLEMENTATION

Our project constituted of the below modules,

- Data Collection
- Dataset
- Importing the necessary libraries
- Clustering(To find Electricity Theft (Target value))
- Splitting the dataset
- Neural network
- Architecture Of ANN
- Apply the model and plot the graphs for accuracy and loss
- Analyze and Prediction

- Accuracy on test set
- Saving the Trained Model

1. Data Collection

In the first module, we do the process of data collection. This is the first real step towards the real development of a machine learning model, collecting data. This is a critical step that will cascade in how good the model will be, the more and better data that we get; the better our model will perform. There are several techniques to collect the data, like web scraping, manual interventions and etc. We have given the dataset in the model folder. The dataset is referred from the popular web repository kaggle. The following is the link to the dataset. Kaggle Dataset Link: https://www.kaggle.com/datasets/jayaprakashpondy/electricity-consumption-dataset

2. Dataset

The dataset consists of 3510433 individual data. There are 9 columns in the dataset which are described below. LCLid: Id number day: Date dd/mm/yyy energy_median: energy medium value energy_mean: energy medium value energy_max: Energy max value energy_count: Energy count value energy_std: Energy std value energy_sum: Energy sum value energy_min: Energy min value

3. Importing the necessary libraries

We will be using Python language for this. First we will import the necessary libraries such as keras for building the main model, sklearn for splitting the training and test data, PIL for converting the images into array of numbers and other libraries such as pandas, numpy ,matplotlib and tensorflow.

4. Clustering

(To find Electricity Theft (Target value)) To find the Electricity Theft using Agglomerative clustering with cluster value = 3 as from our other analysis (base on mean energy).

5. Splitting the dataset

Split the dataset into train and test. 80% train data and 20% test data.

6. Neural network

The second step is to choose a neural network to represent the classification function. For classification problems, it is composed of: A scaling layer. A perceptron layer. A probabilistic layer. For the scaling layer, the minimum and maximum scaling methods are set. We set one perceptron layer, with 3 neurons as a first guess, having the logistic activation function. Neural Network is a series of algorithms that are trying to mimic the human brain and find the relationship between the sets of data. It is being used in various use-cases like in regression, classification, Image Recognition and many more. As we have talked above that neural networks tries to mimic the human brain then there might be the difference as well as the similarity between them. Let us talk in brief about it. Some major differences between them are biological neural network does parallel processing whereas the Artificial neural network does series processing also in the former one processing is slower (in millisecond) while in the latter one processing is faster (in a nanosecond).

7. Architecture of ANN

A neural network has many layers and each layer performs a specific function, and as the complexity of the model increases, the number of layers also increases that why it is known as the multi-layer perceptron. Now in the above picture, you can see each neuron's detailed view. Here, each neurons have some weights (in above picture w1, w2, w3) and biases and based on this computations are done as, combination = bias + weights * input (F = w1*x1 + w2*x2 + w3*x3) and finally activation function is applied output = activation(combination) in above picture activation is sigmoid represented by 1/(1 + e-F). There are some other activation functions as well like ReLU, Leaky ReLU, tanh, and many more. Working of ANN At First, information is feed into the input layer which then transfers it to the hidden layers, and interconnection between these two layers assign weights to each input randomly at the initial point. and then bias is added to each input neuron and after this, the weighted sum which is a combination of weights and bias is passed through the activation function. Activation Function has the responsibility of which node to fire for feature extraction and finally output is calculated. This whole process is known as Foreward Propagation. After getting the output model to compare it with the original output and the error is known and finally, weights are updated in backward propagation to reduce the error and this process continues for a certain number of epochs (iteration). Finally, model weights get updated and prediction is done.

8. Apply the model

Model and plot the graphs for accuracy and loss We will compile the model and apply it using fit function. The batch size will be 64. Then we will plot the graphs for accuracy and loss. We got average training accuracy of 99%.

9. Analyze and Prediction

This module will extract relevant features from the processed data to be used as inputs for the ANN. In the actual dataset, we chose only 7 features : energy_median : energy medium value energy_mean : energy medium value energy_max : Energy max value energy_count : Energy count value energy_std : Energy std value energy_sum : Energy sum value energy_min : Energy min value Target : Unfaithful and Faithful

10. Accuracy

In this module we will evaluate the performance of the developed ANN model on a test dataset to determine its accuracy and effectiveness. We got an accuracy of 99% on test set 4.2.11 Saving the Trained Model Once you're confident enough to take your trained and tested model into the production-ready environment, the first step is to save it into a .h5 or .pkl file using a library like pickle. Make sure you have pickle installed in your environment. Next, let's import the module and dump the model into .pkl file Finally, the trained ANN model will be deployed in a real-world scenario to detect electricity theft using the Web framework flask.

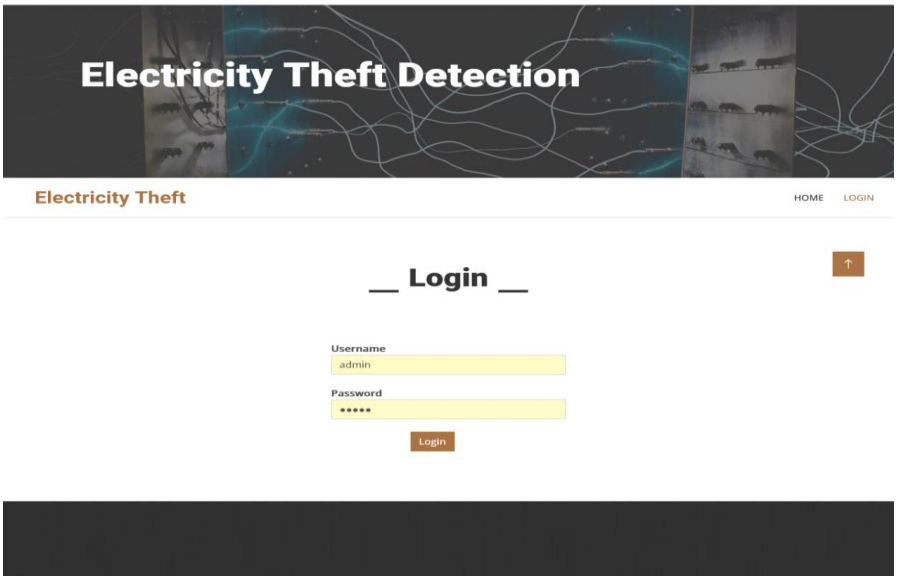
RESULTS AND DISCUSSION :

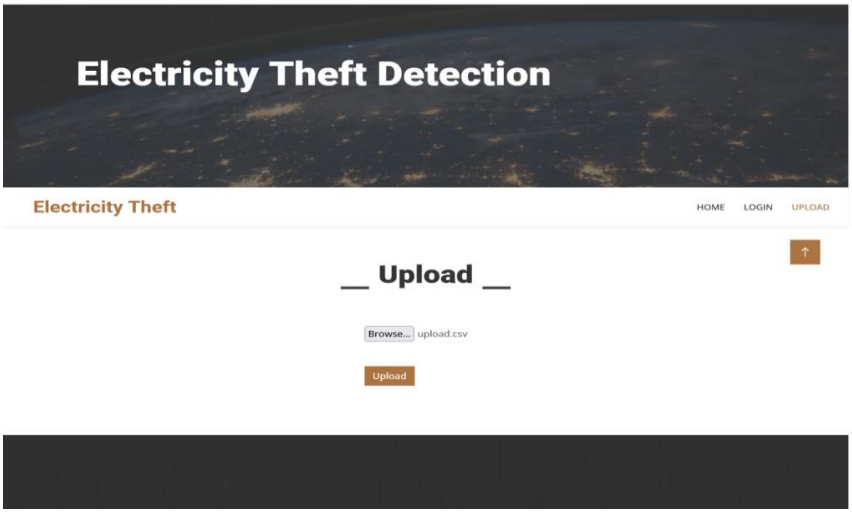
The purpose of testing is to discover errors and ensure that software systems meet their requirements and user expectations without failing in an unacceptable manner. Testing aims to uncover every conceivable fault or weakness in a work product, providing a means to check the functionality of components, sub-assemblies, assemblies, and finished products. Various types of tests address specific testing requirements, including unit testing,

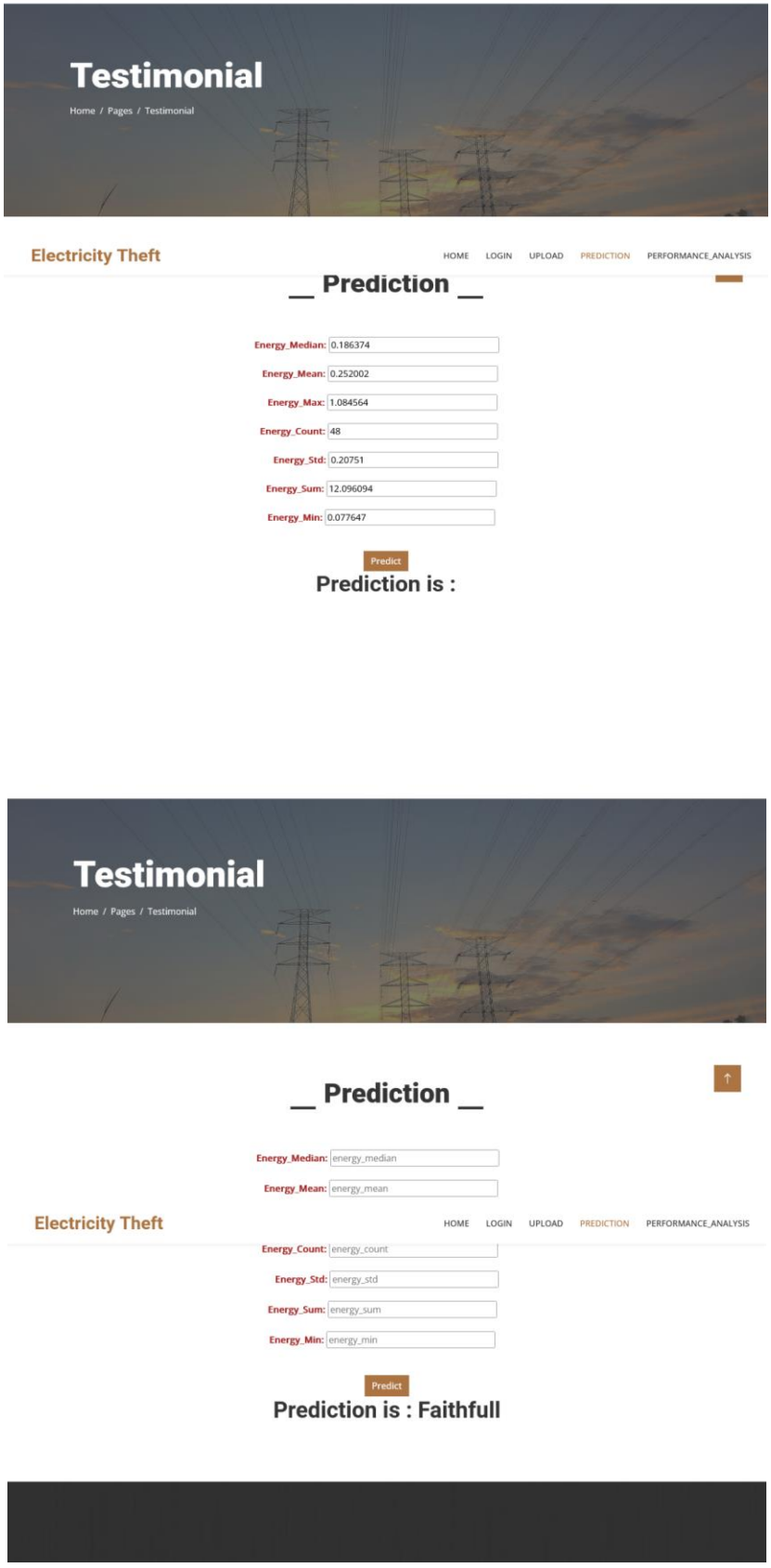
functional testing, acceptance testing, and integration testing. Unit testing focuses on validating internal program logic and ensuring that program inputs produce valid outputs, while functional testing systematically demonstrates that functions are available as specified by business and technical requirements. User acceptance testing (UAT) is critical for confirming that the system meets functional requirements, requiring significant end-user participation. Integration testing ensures that different software components or modules interact correctly and that the system as a whole meets functional and non-functional requirements. By combining these testing strategies, software testing provides comprehensive validation that each unique path of a business process performs accurately, identified inputs and outputs are handled correctly, and interfacing systems or procedures function as expected.

CONCLUSION :

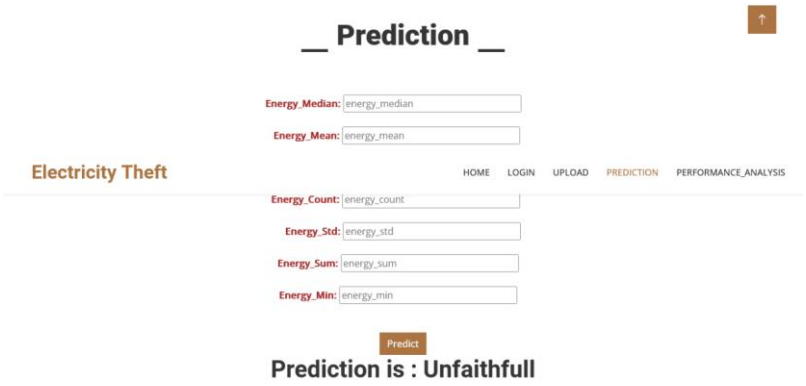
In this work, the detection of electricity theft in smart grids was investigated using Artificial Neural Network (ANN). We observed that classification done with Artificial Neural Network (ANN) is outperformed by classification done with existing system. In our proposed system, we obtained Training Accuracy of 99% and Validation Accuracy of 99%. The method used here utilizes consumption data patterns. Apart from its application in power distribution networks, it can be used in anomaly detection applications in any field. Our work brings a small contribution towards accurately detecting energy theft as we detect theft that only took place over time. In conclusion, the proposed system based on Artificial Neural Network (ANN) has the potential to significantly reduce revenue losses due to electricity theft in smart grids. By detecting instances of theft in real-time and providing alerts to utility companies, the system can help to minimize the impact of electricity theft and improve the overall efficiency and security of the smart grid



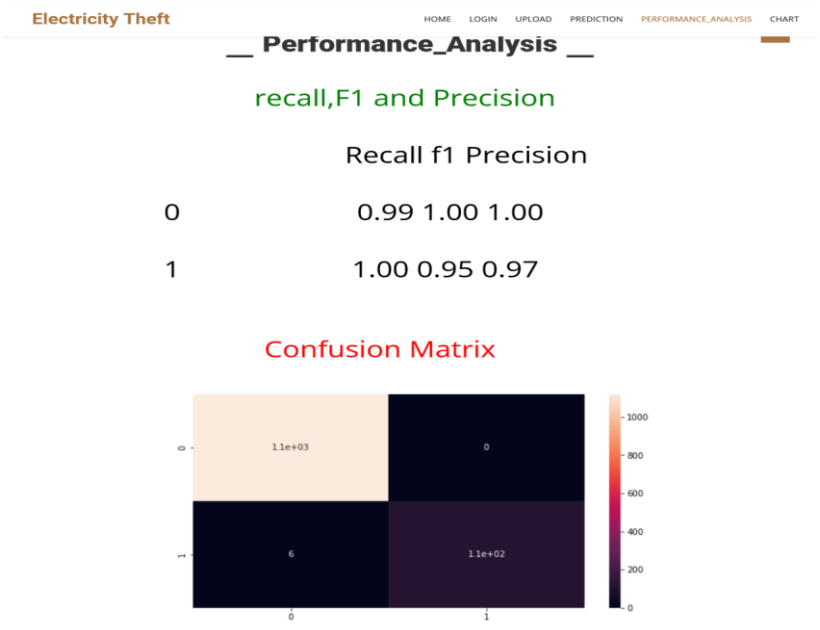



Testimonial
Home / Pages / Testimonial
Electricity Theft
HOME LOGIN UPLOAD PREDICTION PERFORMANCE_ANALYSIS
__ Prediction __
Energy_Median: 0.186374
Energy_Mean: 0.252002
Energy_Max: 1.084564
Energy_Count: 48
Energy_Std: 0.20751
Energy_Sum: 12.096094
Energy_Min: 0.077647
Predict
Prediction is :
Testimonial
Home / Pages / Testimonial
__ Prediction __
Energy_Median: energy_median
Energy_Mean: energy_mean
Electricity Theft
HOME LOGIN UPLOAD PREDICTION PERFORMANCE_ANALYSIS
Energy_Count: energy_count
Energy_Std: energy_std
Energy_Sum: energy_sum
Energy_Min: energy_min
Predict
Prediction is : Faithfull


Testimonial
Home / Pages / Testimonial


__ Prediction __
Energy_Median: energy_median
Energy_Mean: energy_mean
Electricity Theft
HOME LOGIN UPLOAD PREDICTION PERFORMANCE_ANALYSIS
Energy_Count: energy_count
Energy_Std: energy_std
Energy_Sum: energy_sum
Energy_Min: energy_min
Predict
Prediction is : Unfaithfull


Electricity Theft Detection


Electricity Theft
HOME LOGIN UPLOAD PREDICTION PERFORMANCE_ANALYSIS CHART
__ Performance_Analysis __
recall,F1 and Precision
Recall f1 Precision
0 0.99 1.00 1.00
1 1.00 0.95 0.97
Confusion Matrix
1.1e+03
0
6
1.1e+02
1000
800
600
400
200
0

REFERENCE :

[1] J. Astronomo, M. D. Dayrit, C. Edjic, and E. R. T. Regidor, ``Development of electricity theft detector with GSM module and alarm system," in Proc. IEEE 12th Int. Conf. Humanoid, Nanotechnol., Inf. Technol., Commun. Control, Environ., Manage. (HNICEM), Dec. 2020, pp. 15.

[2] M. Anwar, N. Javaid, A. Khalid, M. Imran, and M. Shoaib, ``Electricity theft detection using pipeline in machine learning," in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2020, pp. 21382142.

[3] A. Aldegheishem, M. Anwar, N. Javaid, N. Alrajeh, M. Shaq, and H. Ahmed, ``Towards sustainable energy efciency with intelligent electricity theft detection in smart grids emphasising enhanced neural networks," IEEE Access, vol. 9, pp. 2503625061, 2021.

[4] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, ``Artificial neural networks-based machine learning for wireless networks: A tutorial," 2017, arXiv:1710.02913.

[5] B. Ding, H. Qian, and J. Zhou, ``Activation functions and their characteristics in deep neural networks," in Proc. Chin. Control Decis. Conf. (CCDC), Jun. 2018, pp. 18361841.

[6] I. Diahovchenko, M. Kolcun, Z. ƒonka, V. Savkiv, and R. Mykhailyshyn, ``Progress and challenges in smart grids: Distributed generation, smart metering, energy storage and smart loads," Iranian J. Sci. Technol., Trans. Electr. Eng., vol. 44, no. 4, pp. 13191333, Dec. 2020.

[7] D. O. Dike, U. A. Obiora, E. C. Nwokorie, and B. C. Dike, ``Minimizing household electricity theft in Nigeria using GSM based prepaid meter," Amer. J. Eng. Res., vol. 4, no. 1, pp. 5969, 2015.

[8] P. Dhokane, M. Sanap, P. Anpat, J. Ghuge, and P. Talole, ``Power theft detection & initimate energy meter information through SMS with auto power cut off," Int. J. Current Res. Embedded Syst. VLSI Technol., vol. 2, no. 1, pp. 18, 2017.

[9] S. Foster. (Nov. 2, 2021). Non-Technical Losses: A $96 Billion Global Opportunity for Electrical Utilities. [Online]. Available: https://energycentral.com/c/pip/ non-technical-losses-96-billion-globalopportunity-
electrical-utilities

[10] Q. Louw and P. Bokoro, ``An alternative technique for the detection and mitigation of electricity theft in South Africa," SAIEE Afr. Res. J., vol. 110, no. 4, pp. 209216, Dec. 2019.

[11] Y. Peng, Y. Yang, Y. Xu, Y. Xue, R. Song, J. Kang, and H. Zhao, ``Electricity theft detection in AMI based on clustering and local outlier factor," IEEE Access, vol. 9, pp. 107250107259, 2021.

[12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, ``Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 16061615, Apr. 2018.