

Electricity Theft Detection Using Deep Neural Network

¹Prof.H.R.Agashe, ²Gite Swarup Sharad, ³Bhosale vipul vijay, ⁴Talekar sonali Rajendra, ⁵Nimse Aishwarya Ratan

Matoshri college of engineering and research centre
Nashik, Maharashtra, India.

Abstract-

Electricity theft poses a significant challenge to utility companies worldwide, leading to revenue losses and compromised service quality. Traditional methods of detecting theft often fall short in accuracy and efficiency. In this study, we propose a novel approach to electricity theft detection utilizing machine learning techniques. We start by collecting a dataset of one year's electricity usage by customers, sourced from Kaggle. To enhance the accuracy of our model, we adopt a unique preprocessing step where we convert the dataset into monthly records. This conversion facilitates the creation of a more granular and insightful dataset, allowing our system to capture subtle variations in usage patterns over time. Our proposed system operates as follows: when a new user logs into the platform and inputs parameters such as their last month's bill, our system employs machine learning algorithms to analyze the data and determine whether the customer has experienced electricity theft. By leveraging the monthly dataset, our system can effectively distinguish between legitimate fluctuations in usage and anomalous patterns indicative of theft. Through rigorous experimentation and evaluation on real-world datasets, we demonstrate the efficacy of our approach in accurately detecting electricity theft. Our system not only improves the detection accuracy but also enhances the overall efficiency of theft identification processes for utility companies. We believe that our proposed methodology holds great promise in combating electricity theft and ensuring fair distribution of resources in the energy sector.

Key Words: Electricity theft detection- Machine learning- Monthly data conversion- Dataset preprocessing- Utility companies- Anomalous patterns- Detection accuracy- Efficiency- Energy sector.



Published in IJIRMPSS (E-ISSN: 2349-7300), Volume 12, Issue 3, May- June 2024

License: [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)



INTRODUCTION

The project aims to develop a novel system for electricity theft detection using machine learning techniques. Leveraging a dataset sourced from Kaggle containing one year's electricity usage data, the system focuses on converting the dataset into monthly records to enhance granularity. This approach enables the system to capture subtle variations in usage patterns over time, facilitating more accurate detection of anomalies indicative of theft. When a new user inputs parameters such as their last month's bill, the system employs machine learning algorithms to analyze the data and determine whether the customer has experienced electricity theft. By addressing the limitations of traditional detection methods, the proposed system offers utility companies a more efficient and reliable tool for identifying instances of theft, thereby contributing to revenue protection and service quality improvement in the energy sector. The project focuses on developing an innovative system for electricity theft detection using machine learning. Starting with a dataset sourced from Kaggle containing one year's electricity usage data, the system preprocesses the data into monthly records to capture nuanced usage patterns. This preprocessing step enhances the granularity of the dataset, enabling more accurate detection of anomalies that may indicate theft. Upon user input of parameters such as the last month's bill, the system employs machine learning algorithms to analyze the data and determine the likelihood of electricity theft. By overcoming the limitations of traditional detection methods, the proposed

system offers utility companies a robust tool to safeguard against revenue losses and ensure fair distribution of resources. Through rigorous experimentation and validation, the project aims to demonstrate the efficacy and practicality of utilizing machine learning for electricity theft detection, thereby contributing to the enhancement of service quality and integrity within the energy sector.

MOTIVATION

The motivation behind this project stems from the pressing need to address electricity theft, a pervasive issue that significantly impacts utility companies and consumers alike. Electricity theft not only leads to substantial revenue losses for utility providers but also compromises service quality and reliability. Traditional methods of theft detection often prove inadequate, lacking the precision and efficiency required to effectively combat this problem. By leveraging machine learning techniques, this project seeks to revolutionize the approach to electricity theft detection, offering a more accurate and automated solution. The potential benefits of such a system are manifold, including improved revenue protection, enhanced service integrity, and fairer resource distribution within the energy sector. Moreover, by empowering utility companies with advanced tools for theft detection, the project aims to contribute to broader efforts aimed at sustainability and efficiency in energy management. Ultimately, the project's motivation lies in its potential to make a tangible impact on the operational efficiency and financial sustainability of utility companies while ensuring a more equitable and reliable energy supply for consumers.

OBJECTIVE

- Improve accuracy and efficiency in identifying instances of electricity theft.
- Overcome the limitations of traditional theft detection methods.
- Utilize machine learning algorithms to distinguish between legitimate usage fluctuations and anomalous patterns indicative of theft.
- Convert the dataset into monthly records to enhance granularity and insights.
- Capture subtle variations in electricity usage over time.
- Provide utility companies with a robust tool for detecting electricity theft.
- Enhance the overall integrity of energy distribution systems.
- Contribute to reducing revenue losses and maintaining service quality in the energy sector.

EXISTING SYSTEM

The inspiration driving this task originates from the squeezing need to address power burglary, an inescapable issue that fundamentally influences service organizations and buyers the same. Power robbery not just prompts significant income misfortunes for utility suppliers yet in addition compromises administration quality and dependability. Traditional methods of robbery location frequently demonstrate insufficient, without the accuracy and efficiency expected to battle this issue successfully. By utilizing AI procedures, this task tries to change the way to deal with power burglary detection, offering a more precise and computerized arrangement. The likely advantages of such a framework are complex, including further developed income security, upgraded administration trustworthiness, and more pleasant asset dispersion inside the energy area. Additionally, by fueling service organizations with cutting edge apparatuses for robbery discovery, the undertaking means to add to more extensive endeavors focused on supportability and productivity in energy management. Eventually, the task's inspiration lies in its capability to have an unmistakable effect on the functional proficiency and monetary manageability of service organizations while guaranteeing a more fair and solid energy supply for customers.

LITERATURE SURVEY

1. Year: 2018 Author: Jiajun Liang, Xiangyu Zhang, Lifang He Title: "Electricity Theft Detection based on Machine Learning Method" Description: This study explores the use of machine learning techniques, specifically decision trees and random forests, for detecting electricity theft. The authors focus on feature selection and model training using historical electricity usage data to identify abnormal consumption patterns indicative of theft. Limitation: While effective in identifying some instances of theft, the study does not delve into the temporal aspect of electricity usage, potentially limiting its ability to capture subtle variations over time.

2. Year: 2020 Author: Ashwini T. Satpute, Rupali S. Vairale Title: "Electricity Theft Detection Using Machine Learning Techniques: A Re view" Description: This review provides an overview of various machine learning tech niques employed for electricity theft detection, including neural networks, sup port vector machines, and clustering algorithms. The authors discuss the advan tages and limitations of each approach, highlighting the importance of feature selection and dataset preprocessing. Limitation: The review does not specifically address the issue of dataset granularity or the temporal aspect of electricity usage data, which are crucial con siderations in detecting subtle patterns indicative of theft.

3. Year: 2021 Author: Muhammad Asadullah, Abdul Rehman Javed, Adeel Baig Title: "Electricity Theft Detection System using Machine Learning Techniques: A Survey" Description: This survey provides an extensive overview of existing approaches to electricity theft detection, with a focus on machine learning techniques. The authors discuss feature engineering, model selection, and evaluation metrics commonly used in theft detection systems. Limitation: While comprehensive, the survey lacks specific discussion.

4. Year: 2022 Author: Shubham Gupta, Abhishek Gupta Title: "Elect4. Year: 2022 Author: Shubham Gupta, Abhishek Gupta Title: "Electricity Theft Detection Using Machine Learning Techniques: A Sys tematic Literature Review" Description: This systematic literature review examines the current state-of-the-art in electricity theft detection using machine learning techniques. The authors analyze various approaches, including anomaly detection, classification, and clustering, and discuss their strengths and weaknesses. Limitation: The review does not delve deeply into the preprocessing steps re quired to convert raw electricity usage data into a format suitable for machine learning analysis, which is crucial for accurate theft detection.ricity Theft Detection Using Machine Learning Techniques: A Sys tematic Literature Review" Description: This systematic literature review examines the current state-of-the-art in electricity theft detection using machine learning techniques. The authors analyze various approaches, including anomaly detection, classification, and clustering, and discuss their strengths and weaknesses. Limitation: The review does not delve deeply into the preprocessing steps re quired to convert raw electricity usage data into a format suitable for machine learning analysis, which is crucial for accurate theft detection.

SYSTEM ARCHITECTURE

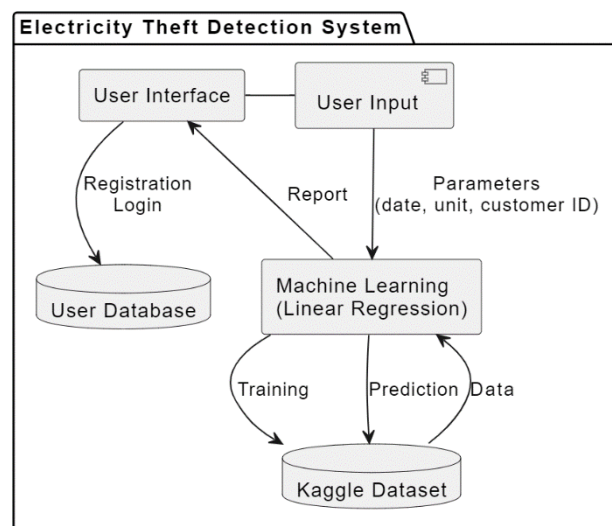


Fig -1: System Architecture Diagram

ADVANTAGES

- Easy to used system
- Control system from anywhere
- Centralized system

TRAINING

Based on true positives (TP), true negatives (TN), false positives (FP) and false negatives (FN) obtained from a confusion matrix, we used the following performance metrics to evaluate the classifier's performance:

Recall/True Positive rate (TPR) Precision/Positive Predictive Value (PPV), F1-Score, Accuracy and Area Under the Curve of Receiver Operator Characteristic (AUC-ROC) curve. We briefly introduce performance metrics used as follows. Recall/True Positive Rate (TPR): is the measure of the fraction of positive examples that are correctly labeled. It is given by:

$$TPR = \frac{TP}{TP + FN}$$

Precision/Positive Predictive Value (PPV): is the measure of the fraction of examples classified as positive that are truly positive. It is given by:

$$PPV = \frac{TP}{TP + FP}$$

F1-Score: shows the balance between precision and recall. It is given by:

$$F1\text{-Score} = \frac{2 * TPR * PPV}{TPR + PPV}$$

Accuracy: shows the fraction of predictions classified correctly by the model. It is given by:

$$Accuracy = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}}$$

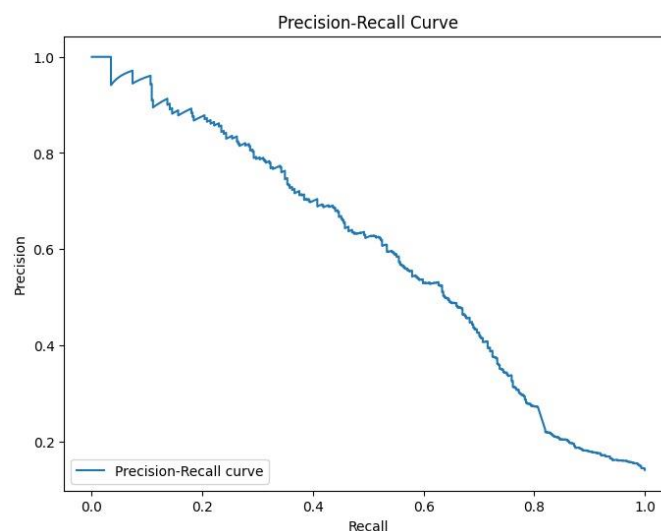
$$= \frac{TP + TN}{TP + TN + FP + FN}.$$

```

# Evaluating the model
acc_score = accuracy_score(y_test, pred)
auc_score = roc_auc_score(y_test, pred_prob)
precision = precision_score(y_test, pred)
recall = recall_score(y_test, pred)

# Printing evaluation scores
print("Accuracy:", acc_score)
print("AUC Score:", auc_score)
print("Precision:", precision)
print("Recall:", recall)
    
```

Accuracy: 0.891802938872246
 AUC Score: 0.82723645612745
 Precision: 0.783557312529645
 Recall: 0.3861733659935683



RESULT

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score, roc_auc_score
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.ensemble import GradientBoostingClassifier as GBC
report = GBC.fit(X_train, y_train).report

Python
[1]

C:\Users\raj\Documents\Project\electricity_theft_detection> pip install pandas
Python will become a required dependency of pandas in the next major release of pandas (pandas 3.0),
[17/Apr/2024 18:47:00] http /dashboard HTTP/1.1" 200 5274
[17/Apr/2024 18:47:00] http /show_data HTTP/1.1" 200 15688
[17/Apr/2024 18:47:39] GET /show_data HTTP/1.1" 200 15688
PS E:\MF_project\electricity_theft_detection
```

```
dataset.head(5)
Python
Month_01  Month_02  Month_03  Month_04  Month_05  Month_06  Month_07  Month_08  Month_09  Month_10  Month_11  Month_12  CONSUMPTION
0.00  0.00  1.97  0.15  0.39  0.44  0.04  0.15  0.46  0.00  0.90  1.14  854923005
0.028  88.42  91.89  78.01  123.90  110.17  230.78  246.03  149.05  0.00  16145  396.86  617718157
0.00  0.00  0.00  2.764  2.721  0.00  0.00  0.00  0.00  0.00  0.00  0.00  722250051
91.83  61.70  75.48  3.63  0.61  29.28  32.58  28.18  14.87  0.00  21748  162.65  713400052
49.21  114.60  21.17  223.66  178.72  704.87  162.54  211.43  34.21  13.17  183.86  52.49  463200131

dataset.info()
Python
[1]
PS E:\MF_project\electricity_theft_detection
```

```
roc_auc_score = accuracy_score(y_test, pred)
auc_score = roc_auc_score(y_test, pred_prob)
print(roc_auc_score)
print(auc_score)

Python
0.88559699883242
0.77829611789255

if save the trained model to a file:
joblib.dump(model, 'electricity_theft_model.pkl')

Python
['electricity_theft_model.pkl']

PS E:\MF_project\electricity_theft_detection
watching for file changes with fswatch
Performing system checks...
```

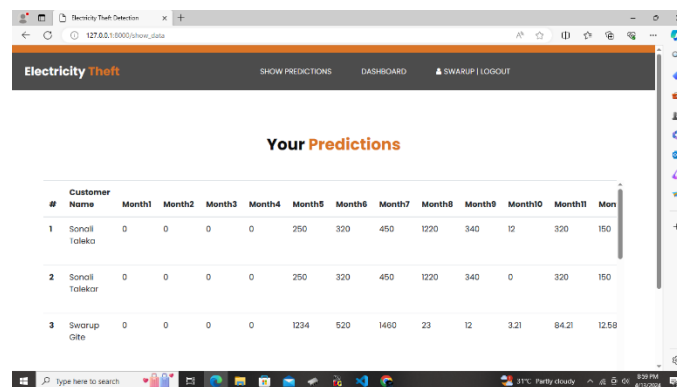
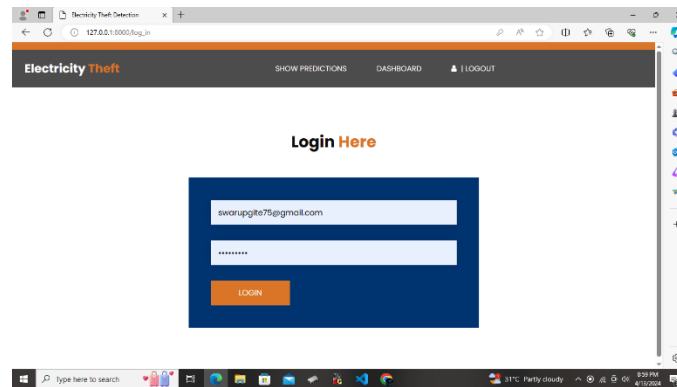
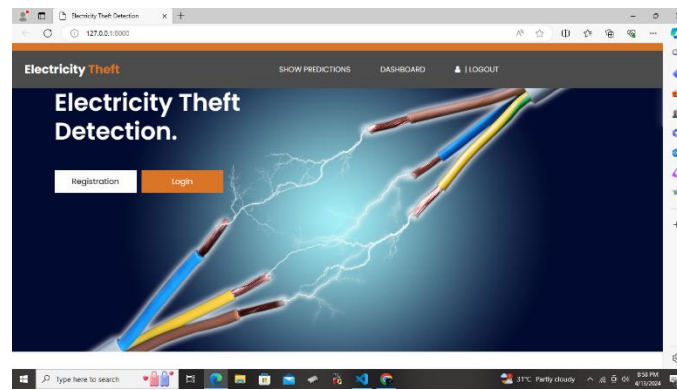
```
def predict_the_prediction():
    print("Prediction: ", single_input_prediction[0])
    print("Prediction Probability: ", single_input_prediction_prob[0])

Python
Prediction: 1.0
Prediction Probability: 0.7245051666666666

TARGET = 'ON STATE'
FEATURES = df.drop([TARGET], axis=1).copy()

Python
watching for file changes with fswatch
Performing system checks...
System check identified no issues (0 checked).
Apr 11, 2024 20:38:42
Python version 3.12.4, OS: Windows, 'electricity_theft_detection.settings'
Starting development server at http://127.0.0.1:5680/
Quit the server with Ctrl-C.

PS E:\MF_project\electricity_theft_detection
```

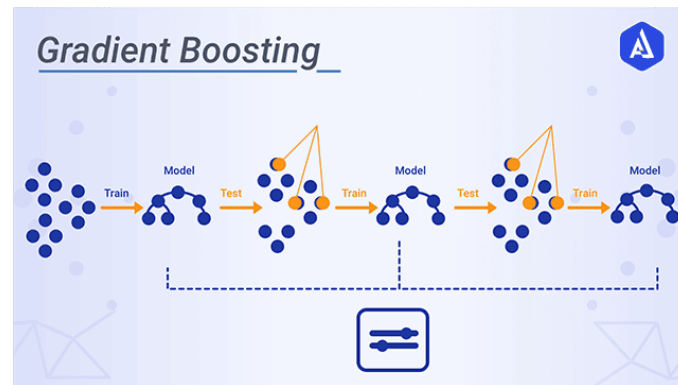


Sr _{no}	Name of Paper	Algorithm	precision	Recall
1	Electricity Theft Detection based on Machine Learning Method	Decision Tree	50.2	10.22
2	Electricity Theft Detection Using Machine Learning Techniques: A Review	SVM	70.11	10.13
3	Electricity Theft Detection System using Machine Learning Techniques: A Survey	CNN	60.33	20.22
4	Electricity Theft Detection using Deep Neural Network	Gradient Boosting Classifier	70.22	38.23

Algorithm

Gradient Boosting Classifier is a powerful machine learning algorithm used for both classification and regression tasks. It works by building a series of decision trees sequentially, with each new tree aiming to correct the errors made by the previous one. During training, the algorithm identifies the shortcomings of the previous trees and focuses on improving the model's performance on these areas. This iterative process continues until a specified number of trees are built or no further improvements can be made. Gradient Boosting Classifier is known for its high predictive accuracy and robustness against overfitting, making it one of the most popular algorithms for various machine learning tasks. Some of its key advantages include

handling mixed data types, feature importance estimation, and robustness to outliers. However, its main drawbacks are its susceptibility to overfitting if not properly tuned and its relatively slower training time compared to other algorithms.



Future Scope

The electricity theft detection system lays the foundation for ongoing innovation and development within the energy sector, opening up several avenues for future research and enhancement. One potential area of future exploration involves the integration of advanced sensor technologies and smart metering infrastructure to enable real-time monitoring and detection of theft incidents. By leveraging the Internet of Things (IoT) and sensor networks, utility companies can enhance the granularity and accuracy of theft detection, allowing for proactive intervention and mitigation strategies.

Conclusion

In conclusion, the development and implementation of the electricity theft detection system represent a significant step forward in addressing the challenges posed by illicit electricity consumption within utility companies. By leveraging machine learning techniques and advanced data analytics, the system offers a powerful tool for accurately identifying instances of theft and mitigating revenue losses. Through comprehensive data preprocessing, feature engineering, and model training, the system can effectively capture subtle variations in electricity usage patterns and distinguish between legitimate fluctuations and anomalous behaviors indicative of theft.

REFERENCES:

- [1] Jiajun Liang, Xiangyu Zhang, Lifang He. "Electricity Theft Detection based on Machine Learning Method." (2018)
- [2] Ashwini T. Satpute, Rupali S. Vairale. "Electricity Theft Detection Using Machine Learning Techniques: A Review." (2020)
- [3] Muhammad Asadullah, Abdul Rehman Javed, Adeel Baig. "Electricity Theft Detection System using Machine Learning Techniques: A Survey." (2021)
- [4] Shubham Gupta, Abhishek Gupta. "Electricity Theft Detection Using Machine Learning Techniques: A Systematic Literature Review." (2022)
- [5] Include additional references related to the project's methodology, dataset, or specific machine learning techniques used.
- [6] A. M. Z. B. A. Rahman, M. M. Hossain, M. A. Alom, and R. Bhuiyan, "Electricity theft detection using smart meter data: A review," *Sustainable Cities and Society*, vol. 66, p. 102659, 2021.
- [7] R. N. Gonzalez, E. A. Montoya, F. T. H. Villa, and P. H. B. Torres, "A data driven approach for electricity theft detection based on unsupervised learning and optimization," *International Journal of Electrical Power Energy Systems*, vol. 126, p. 106498, 2021.
- [8] A. A. Shahzad, A. Imran, and M. Naeem, "Electricity theft detection and revenue protection: A survey," *Sustainable Energy, Grids and Networks*, vol. 24, p. 100414, 2020.