International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Electricity theft detection in smart grids based on DL

Ms.Ch.Usha Maheshwari[1], Medari Bhavika[2], Matapathi Shashanka[3], Majjiga shreshta[4]
[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India.
[2,3,4]UG-Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India.

ABSTRACT

As one of the major factors of the nontechnical losses (NTLs) in distribution networks, the electricity theft causes significant harm to power grids, which influences power supply quality and reduces operating profits. In order to help utility companies solve the problems of inefficient electricity inspection and irregular power consumption, a novel hybrid convolutional neural network-random forest (CNN-RF) model for automatic electricity theft detection is presented in this paper. In this model, a convolutional neural network (CNN) firstly is designed to learn the features between different hours of the day and different days from massive and varying smart meter data by the operations of convolution and down-sampling. In addition, a dropout layer is added to retard the risk of overfitting, and the backpropagation algorithm is applied to update network parameters in the training phase. And then, the random forest (RF) is trained based on the obtained features to detect whether the consumer steals electricity. To build the RF in the hybrid model, the grid search algorithm is adopted to determine optimal parameters. Finally, experiments are conducted based on real energy consumption data, and the results show that the proposed detection model outperforms other methods in terms of accuracy and efficiency.

INDEX TERMS: Deep neural network, electricity theft, machine learning, minimum redundancy maximum relevance, principal component analysis, smart grids.

INTRODUCTION

The loss of energy in electricity transmission and distribution is an important problem faced by power companies all over the world. The energy losses are usually classified into technical losses (TLs) and non technical losses (NTLs) [1]. The TL is inherent to the transportation of electricity, which is caused by interna actions in the power system components such as the transmission liner and transformers [2]; the NTL is defined as the difference between total losses and (TLs), which is primarily caused by electricity theft. Actually, the electricity theft occurs mostly through physical attacks like line tapping, meter breaking, or meter reading tampering[3]. These electricity fraud behaviour may bring about the revenue loss of power companies. As an example, the losses caused by electricity theft are estimated as about $4.5 billion every year in the United States(US) [4]. And it is estimated that utility companies worldwide lose more than 20 billion every year in the form of electricity theft [5]. In addition, electricity theft behaviours can also affect the power system safety. For instance, the heavy load of electrical systems caused by electricity theft may lead to fires, which threaten the public safety. Therefore, accurate electricity theft detection is crucial for power grid safety and stableness.

With the implementation of the advanced metering infrastructure (AMI) in smart grids, power utilities obtained massive amounts of electricity consumption data at a high frequency from smart meters, which is helpful for us to detect electricity theft. However, every coin has two sides; the AMI network opens the door for some new electricity theft attacks. These attacks in the AMI can be launched by various means such as digital tools and cyber attacks. The primary means of electricity theft detection include humanly examining unauthorized line diversions, comparing malicious meter records with the benign ones, and checking problematic equipment or hardware. However, these methods are extremely time consuming and costly during full verification of all meters in a system. Besides, these manual approaches cannot avoid cyber attacks. In order to solve the problems mentioned above, many approaches have been put forward in the past years.

These methods are mainly categorized into state-based, game-theory-based, and artificial intelligent models.

Deep learning techniques for electricity theft detection are studied in [18], where the authors present a comparison between different deep learning architectures such as convolutional neural networks (CNNs), long-short-term memory (LSTM) recurrent neural networks (RNNs), and stacked autoencoders. However, the performance of the detectors is investigated using synthetic data, which does not allow a reliable assessment of the detector’s performance compared with shallow architectures. Moreover, the authors in [19] proposed a deep neural network- (DNN-) based customer-specific detector that can efficiently thwart such cyber attacks. In recent years, the CNN has been applied to generate useful and discriminative features from raw data and has wide applications in different areas [20–22]. These applications motivate the CNN applied for feature extraction from high-resolution smart meter data in electricity theft detection. In [23], a wide and deep convolutional neural network (CNN) model was developed and applied to analyze the electricity theft in smart grids.

1.EXISITING SYSTEM

Research on electricity theft detection in smart grids has attracted many researchers to devise methods that mitigate against electricity theft. Methods used in the literature can be broadly categorized into the following three categories: hardware-based, combined hardware and data-based detection methods and data-driven methods. Hardware-based methods generally require hardware devices such as specialized microcontrollers, sensors and circuits to be installed on power distribution lines. Electricity cyberattack is a form of electricity theft whereby energy consumption data is modified by hacking the electricity meters.

The electricity consumption data is frequently incorrect and loud, several traditional methods of data investigation, e.g., Support Vector Machine(SVM) cannot be straight carried out to the consumption of electricity data because of the calculation difficulty and the restricted simplification ability. Thus, to face the above challenges, the DNN approach has been adopted in this work.

2.PROPOSED SYSTEM

The electricity theft detection method outlined consists of the following three steps: Data Analysis and Pre-processing, Feature Extraction, and Classification. Implementation of smart grids comes with many opportunities to solve the electricity theft problem. Smart grids are usually composed of traditional power grids, smart meters and sensors, computing facilities to monitor and control grids, etc., all connected through the communication network. Deep Neural Network techniques that have been built to imitate biological human brain mechanisms. They are typically used for extracting patterns or detecting trends that are difficult to be detected by other machine learning techniques.

REQUIREMENT ANALYSIS

The project involved analyzing the design of few applications to make the application more users friendly. To do so, it was important to keep the navigations from one screen to the other well- ordered and at the same time reducing the amount of typing the user needs to do. To make the application more accessible, the browser version had to be chosen so that it is compatible with most of the Browsers.

SYSTEM REQUIREMENTS

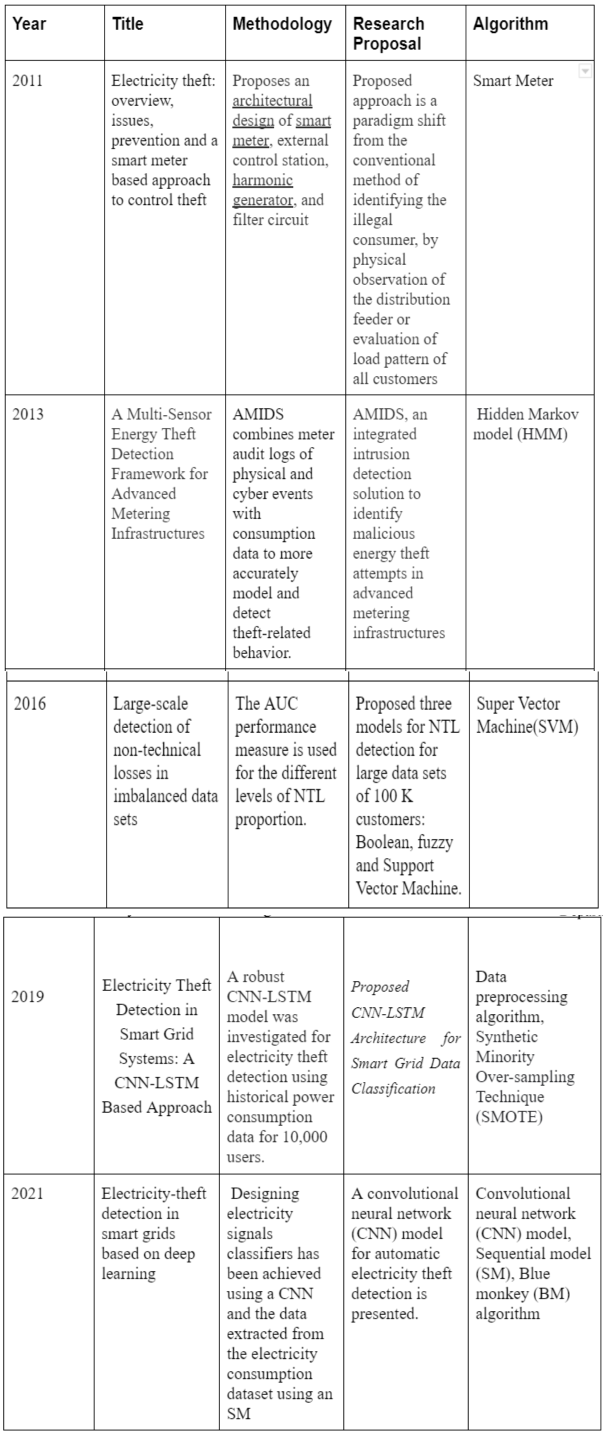
HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- **Operating System:** Windows
- **Coding Language**: Python 3.7
- **Front End** : Python

LITERATURE REVIEW:



Year	Title	Methodology	Research Proposal	Algorithm
2011	Electricity theft: overview, issues, prevention and a smart meter based approach to control theft	Proposes an architectural design of smart meter, external control station, harmonic generator, and filter circuit	Proposed approach is a paradigm shift from the conventional method of identifying the illegal consumer, by physical observation of the distribution feeder or evaluation of load pattern of all customers	Smart Meter
2013	A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures	AMIDS combines meter audit logs of physical and cyber events with consumption data to more accurately model and detect theft-related behavior.	AMIDS, an integrated intrusion detection solution to identify malicious energy theft attempts in advanced metering infrastructures	Hidden Markov model (HMM)
2016	Large-scale detection of non-technical losses in imbalanced data sets	The AUC performance measure is used for the different levels of NTL proportion.	Proposed three models for NTL detection for large data sets of 100 K customers: Boolean, fuzzy and Support Vector Machine.	Super Vector Machine(SVM)
2019	Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach	A robust CNN-LSTM model was investigated for electricity theft detection using historical power consumption data for 10,000 users.	*Proposed CNN-LSTM Architecture for Smart Grid Data Classification*	Data preprocessing algorithm, Synthetic Minority Over-sampling Technique (SMOTE)
2021	Electricity-theft detection in smart grids based on deep learning	Designing electricity signals classifiers has been achieved using a CNN and the data extracted from the electricity consumption dataset using an SM	A convolutional neural network (CNN) model for automatic electricity theft detection is presented.	Convolutional neural network (CNN) model, Sequential model (SM), Blue monkey (BM) algorithm

INPUT DESIGN:

- The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data into a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:
- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES:

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2.It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus, the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

1. A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.
2. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

3.Select methods for presenting information.
4.Create document, report, or other formats that contain information produced by the system.
1.The output form of an information system should accomplish one or more of the
following objectives.

- Convey information about past activities, status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.

METHODOGY

Deep Learning

Deep learning is a branch of machine learning. Unlike traditional machine learning algorithms, many of which have a finite capacity to learn no matter how much data they acquire, deep learning systems can improve their performance with access to more data: the machine version of more experience. After machines have gained enough experience through deep learning, they can be put to work for specific tasks such as driving a car, detecting weeds in a field of crops, detecting diseases, inspecting machinery to identify faults, and so on.

How does deep learning work?

Deep learning networks learn by discovering intricate structures in the data they experience.

By building computational models that are composed of multiple processing layers, the networks can create multiple levels of abstraction to represent the data. Deep learning is fundamentally different from conventional machine learning.

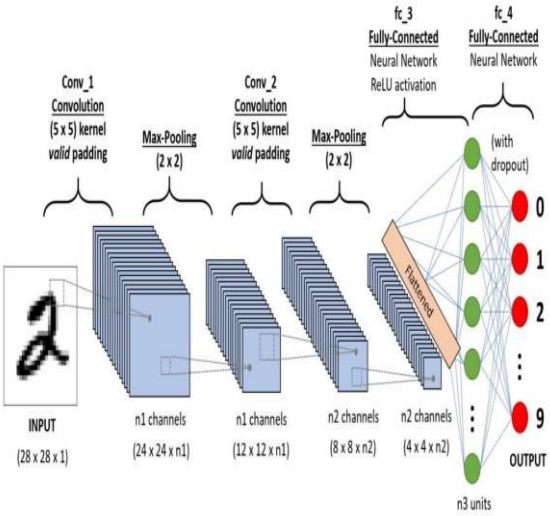
For example, a deep learning model known as a convolutional neural network can be trained using large numbers (as in millions) of images, such as those containing cats. This type of neural network typically learns from the pixels contained in the images it acquires. It can classify groups of pixels that are representative of a cat’s features, with groups of features such as claws, ears, and eyes indicating the presence of a cat in an image.
Deep learning is fundamentally different from conventional machine learning. In this example, a domain expert would need to spend considerable time engineering a conventional machine learning system to detect the features that represent a cat. With deep learning, all that is needed is to supply the system with a very large number of cat images, and the system can autonomously learn the features that represent a cat.

ALGORITHMS:

Convolutional Neural Network(CNN)

A **Convolutional Neural Network (Conv Net/CNN)** is a Deep Learning algorithm that can take in an input image, assign importance (learnable weights and biases) to various aspects/objects in the image, and be able to differentiate one from the other. The pre-processing required in a Conv Net is much lower as compared to other classification algorithms. While in primitive methods filters are hand-engineered, with enough training, Conv Nets have the ability to learn these filters/characteristics.

The architecture of a Conv Net is analogous to that of the connectivity pattern of Neurons in the Human Brain and was inspired by the organization of the Visual Cortex. Individual neurons respond to stimuli only in a restricted region of the visual field known as the Receptive Field. A collection of such fields overlap to cover the entire visual area.

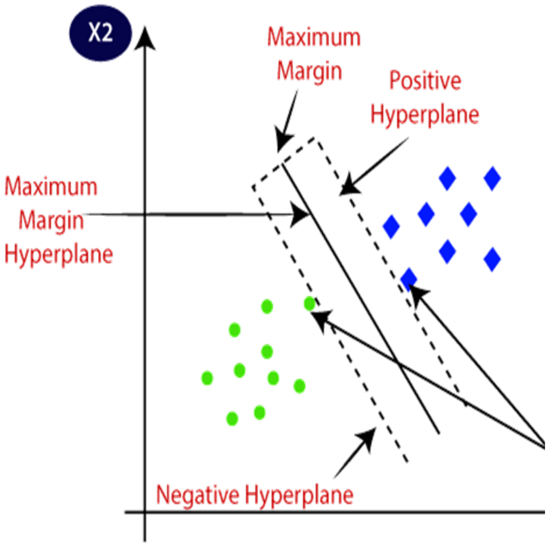


Support Vector Machine (SVM)

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning.

The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane.

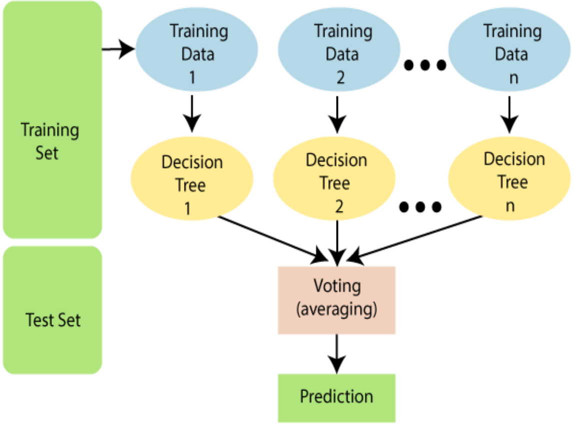
SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine. Consider the below diagram in which there are two different categories that are classified using a decision boundary or hyperplane:



Random Forest

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of ensemble learning, which is a process of combining multiple classifiers to solve a complex problem and to improve the performance of the model.

As the name suggests, "Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output.



Logistic regression competes with discriminant analysis as a method for analysing categorical response variables. Many statisticians feel that logistic regression is more versatile and better suited for modelling most situations than is discriminant analysis. This is because logistic regression does not assume that the independent variables are normally distributed, as discriminant analysis does.

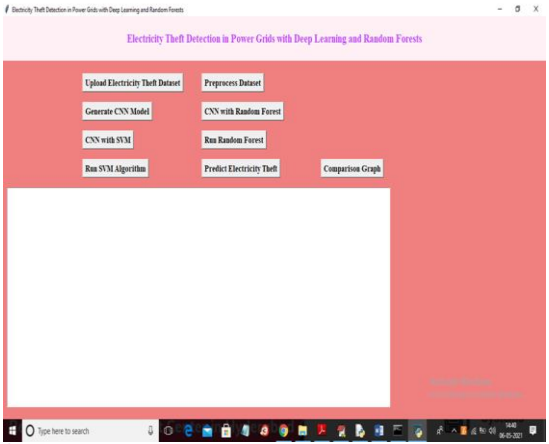
This program computes binary logistic regression and multinomial logistic regression on both numeric and categorical independent variables. It reports on the regression equation as well as the goodness of fit, odds ratios, confidence limits, likelihood, and deviance. It performs a comprehensive residual analysis including diagnostic residual reports and plots. It can perform an independent variable subset selection search, looking for the best regression model with the fewest independent variables. It provides confidence intervals on predicted values and provides ROC curves to help determine the best cut off point for classification. It allows you to validate your results by automatically classifying rows that are not used during the analysis.

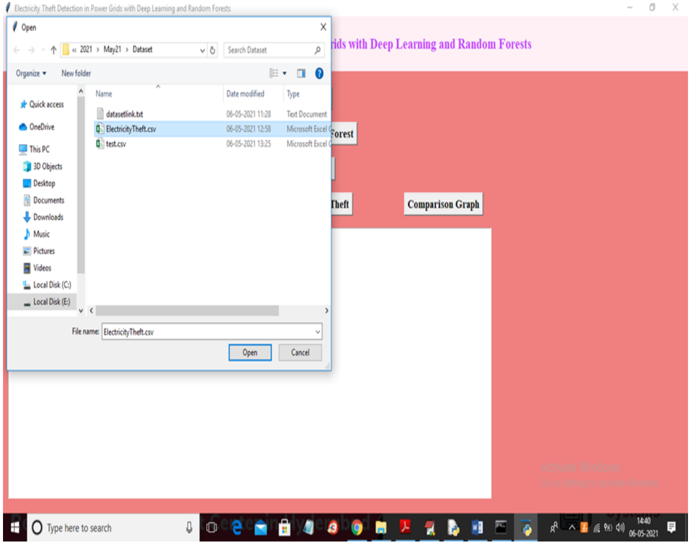
CONCLUSION:

In this work, the detection of electricity theft in smart grids was investigated using time-domain and frequency-domain features in a DNN-based classification approach. Isolated classification tasks based on the time-domain, frequencydomain and combined domains features were investigated on the same DNN network. Widely accepted performance metrics such as recall, precision, F1-score, accuracy, AUCROC and MCC were used to measure the performance of the model. We observed that classification done with frequency-domain features outperforms classification done with time-domain features, which in turn is outperformed by classification done with features from both domains. The classifier was able to achieve 87.3% accuracy and 93% AUC-ROC when tested. We used PCA for feature reduction. With 7 out of 20 components used, the classifier was able to achieve 85.8% accuracy and 92% AUC-ROC when tested. We further analyzed individual features' contribution to the classification task and confirmed with the mRMR algorithm the importance of frequency-domain features over time-domain features towards a successful classification task. For better performance, a Bayesian optimizer was also used to optimize hyperparameters, which realized accuracy improvement close to 1%, on validation. Adam optimizer was incorporated and optimal values of key parameters were investigated. In comparison with other data-driven methods evaluated on the same dataset, we obtained 97% AUC which is 1% higher than the best AUC in existing works, and 91.8% accuracy, which is the second-best on the benchmark. 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. We wish to extend our method to detect real-time electricity theft in the future. Since this method was evaluated based on consumption patterns of SGCC customers, it can further be validated against datasets from different areas to ensure its applicability anywhere.

RESULT AND ANALYSIS:

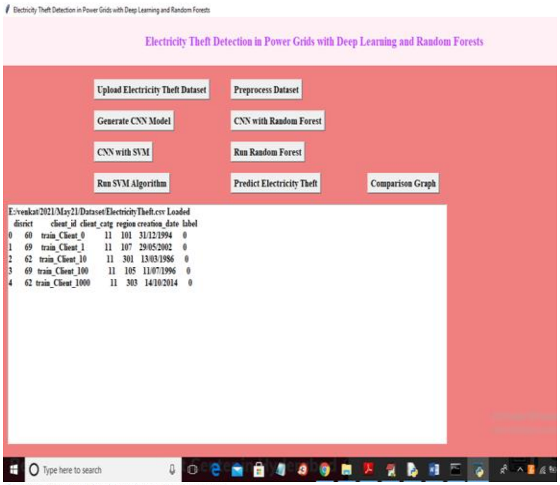
SCREENSHOTS:


Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search
14:40
06-05-2021

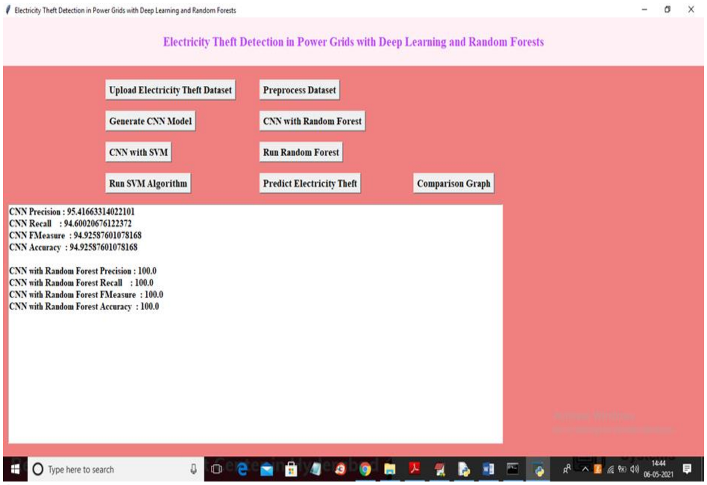


Name	Date modified	Type
datasetlink.txt	06-05-2021 11:28	Text Document
ElectricityTheft.csv	06-05-2021 12:58	Microsoft Excel C
test.csv	06-05-2021 13:25	Microsoft Excel C

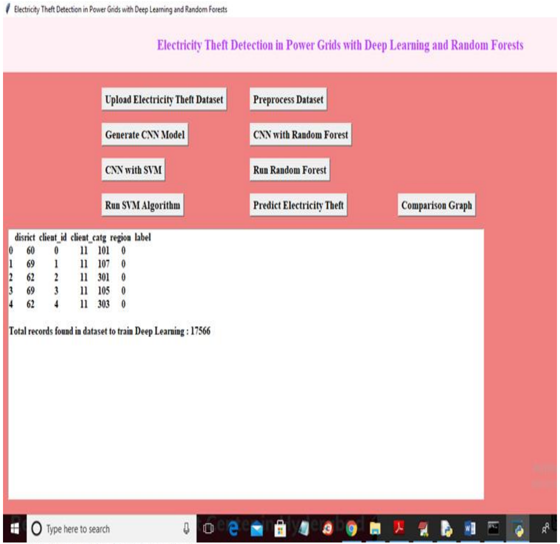
File name: ElectricityTheft.csv


Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search

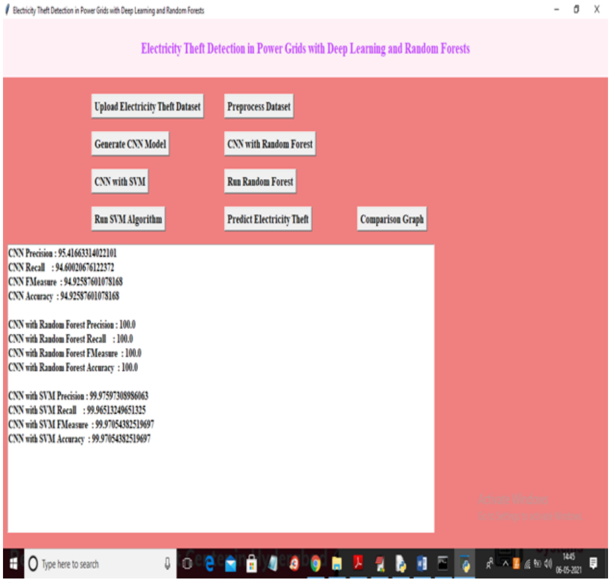
```
E:/venkat/2021/May21/Dataset/ElectricityTheft.csv Loaded
  disrict        client_id  client_catg  region creation_date  label
0      60     train_Client_0         11     101    31/12/1994     0
1      69     train_Client_1         11     107    29/05/2002     0
2      62    train_Client_10         11     301    13/03/1986     0
3      69   train_Client_100         11     105    11/07/1996     0
4      62  train_Client_1000         11     303    14/10/2014     0
```


Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search

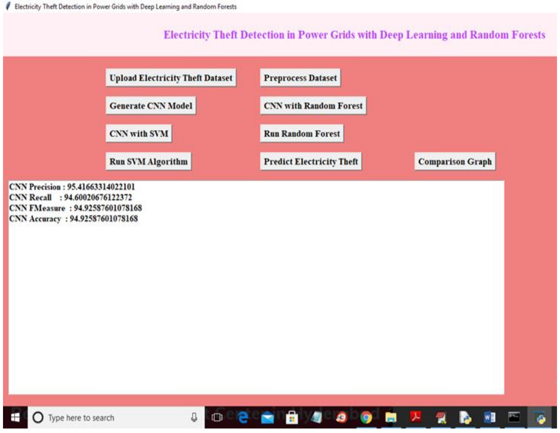
```
CNN Precision : 95.41663314022101
CNN Recall    : 94.60020676122372
CNN FMeasure  : 94.92587601078168
CNN Accuracy  : 94.92587601078168

CNN with Random Forest Precision : 100.0
CNN with Random Forest Recall    : 100.0
CNN with Random Forest FMeasure  : 100.0
CNN with Random Forest Accuracy  : 100.0
```


Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search

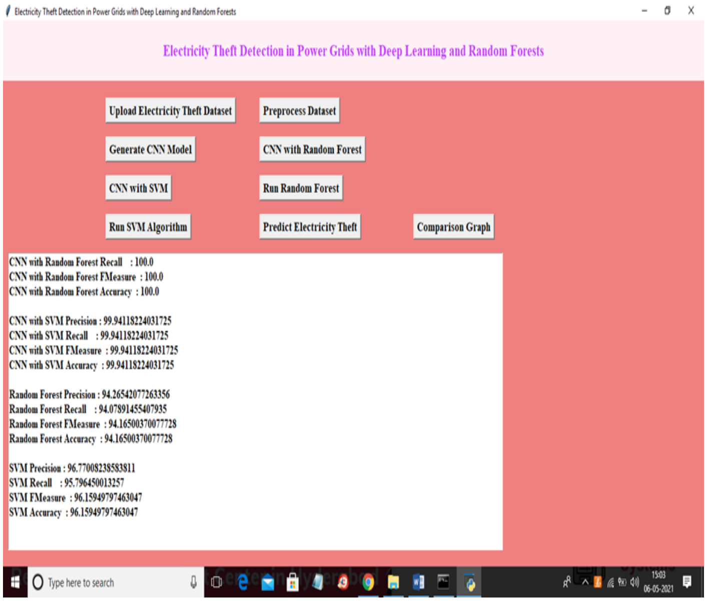
```
  disrict  client_id  client_catg  region  label
0      60          0           11     101      0
1      69          1           11     107      0
2      62          2           11     301      0
3      69          3           11     105      0
4      62          4           11     303      0

Total records found in dataset to train Deep Learning : 17566
```


Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search

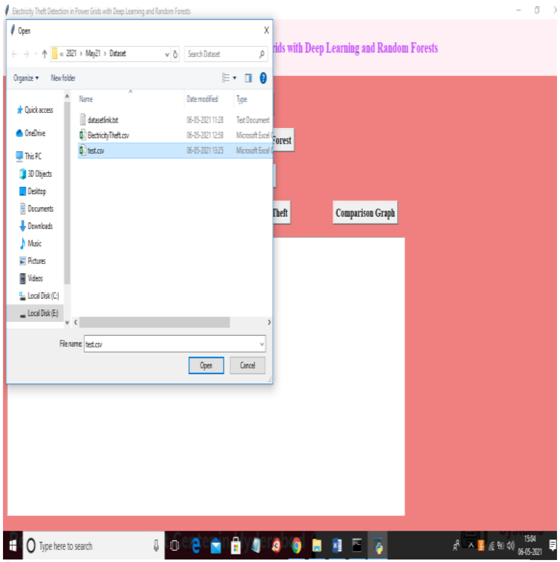
```
CNN Precision : 95.41663314022101
CNN Recall    : 94.60020676122372
CNN FMeasure  : 94.92587601078168
CNN Accuracy  : 94.92587601078168

CNN with Random Forest Precision : 100.0
CNN with Random Forest Recall    : 100.0
CNN with Random Forest FMeasure  : 100.0
CNN with Random Forest Accuracy  : 100.0

CNN with SVM Precision : 99.97597308986063
CNN with SVM Recall    : 99.96513249651325
CNN with SVM FMeasure  : 99.97054382519697
CNN with SVM Accuracy  : 99.97054382519697
```


Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search

```
CNN Precision : 95.41663314022101
CNN Recall    : 94.60020676122372
CNN FMeasure  : 94.92587601078168
CNN Accuracy  : 94.92587601078168
```

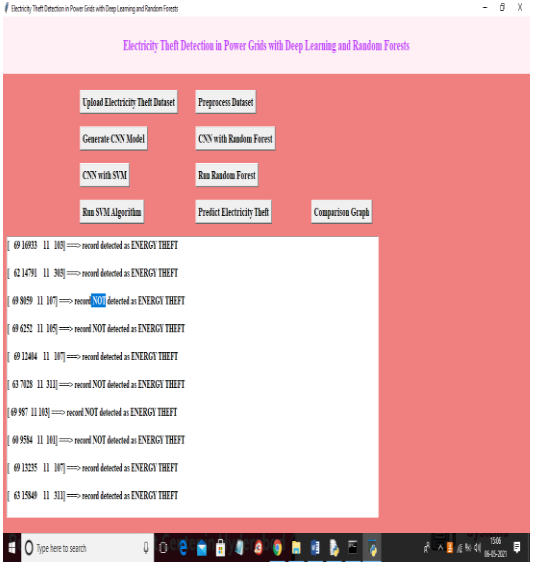

Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Electricity Theft Detection in Power Grids with Deep Learning and Random Forests
Upload Electricity Theft Dataset
Preprocess Dataset
Generate CNN Model
CNN with Random Forest
CNN with SVM
Run Random Forest
Run SVM Algorithm
Predict Electricity Theft
Comparison Graph
Type here to search

```
CNN with Random Forest Recall    : 100.0
CNN with Random Forest FMeasure  : 100.0
CNN with Random Forest Accuracy  : 100.0

CNN with SVM Precision : 99.94118224031725
CNN with SVM Recall    : 99.94118224031725
CNN with SVM FMeasure  : 99.94118224031725
CNN with SVM Accuracy  : 99.94118224031725

Random Forest Precision : 94.26542077263356
Random Forest Recall    : 94.07891455407935
Random Forest FMeasure  : 94.16500370077728
Random Forest Accuracy  : 94.16500370077728

SVM Precision : 96.7700823858381l
SVM Recall    : 95.796450013257
SVM FMeasure  : 96.1594979746304 7
SVM Accuracy  : 96.1594979746304 7
```

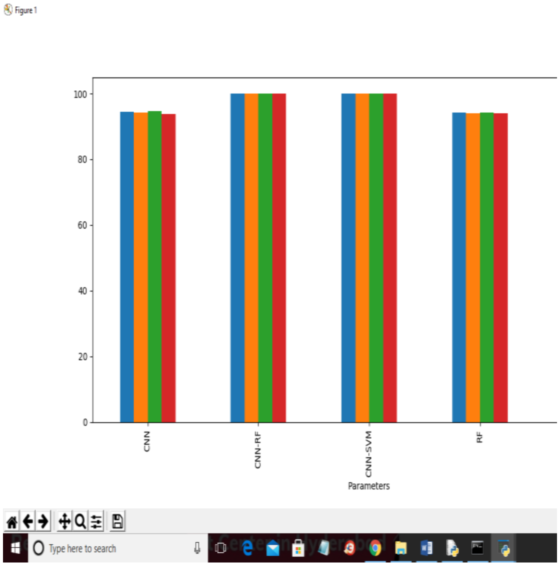


Name	Date modified	Type
datasetlink.txt	06-05-2021 11:28	Text Document
ElectricityTheft.csv	06-05-2021 12:58	Microsoft Excel
test.csv	06-05-2021 13:25	Microsoft Excel

File name: test.csv



```
[  69 16933   11   103] ==> record detected as ENERGY THEFT
[  62 14791   11   303] ==> record detected as ENERGY THEFT
[ 69 8059   11  107] ==> record NOT detected as ENERGY THEFT
[ 69 6252   11  105] ==> record NOT detected as ENERGY THEFT
[  69 12404   11   107] ==> record detected as ENERGY THEFT
[ 63 7028   11  311] ==> record NOT detected as ENERGY THEFT
[ 69 987  11 103] ==> record NOT detected as ENERGY THEFT
[ 60 9584   11  101] ==> record NOT detected as ENERGY THEFT
[  69 13235   11   107] ==> record detected as ENERGY THEFT
[  63 15849   11   311] ==> record detected as ENERGY THEFT
```



CONCLUSION:

In this paper, a novel CNN-RF model is presented to detect electricity theft. In this model, the CNN is similar to an automatic feature extractor in investigating smart meter data and the RF is the output classifier. Because a large number of parameters must be optimized that increase the risk of overfitting, a fully connected layer with a dropout rate of 0.4 is designed during the training phase. In addition, the SMOT algorithm is adopted to overcome the problem of data imbalance. Some machine learning and deep learning methods such as SVM, RF, GBDT, and LR are applied to the same problem as a benchmark, and all those methods have been conducted on SEAI and LCL datasets. The results indicate that the proposed CNN-RF model is quite a promising classification method in the electricity theft detection field because of two properties: The first is that features can be automatically extracted by the hybrid model, while the success of most other traditional classifiers relies largely on the retrieval of good hand-designed features which is a laborious and time-consuming task. The second lies in that the hybrid model combines the advantages of the RF and CNN, as both are the most popular and successful classifiers in the electricity theft detection field.

Since the detection of electricity theft affects the privacy of consumers, the future work will focus on investigating how the granularity and duration of smart meter data might affect this privacy. Extending the proposed hybrid CNN-RF model to other applications (e.g., load forecasting) is a task worth investigating.

REFERENCES:

[1] 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

[2] 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. 209–216, Dec. 2019.

[3] 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. 2138–2142.

[4] 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. 1606–1615, Apr. 2018.

[5] P. Pickering. (Nov. 1, 2021). E-Meters Offer Multiple Ways to Combat Electricity Theft and Tampering. [Online]. Available: https://www.electronicdesign.com/technologies/meters

[6] X. Fang, S. Misra, G. Xue, and D. Yang, ‘‘Smart grid—The new and improved power grid: A survey,’’ IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[7] M. Ismail, M. Shahin, M. F. Shaaban, E. Serpedin, and K. Qaraqe, ‘‘Efficient detection of electricity theft cyber attacks in AMI networks,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1–6.

[8] A. Maamar and K. Benahmed, ‘‘Machine learning techniques for energy theft detection in AMI,’’ in Proc. Int. Conf. Softw. Eng. Inf. Manage. (ICSIM), 2018, pp. 57–62.

[9] A. Jindal, A. Schaeffer-Filho, A. K. Marnerides, P. Smith, A. Mauthe, and L. Granville, ‘‘Tackling energy theft in smart grids through data-driven analysis,’’ in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2020, pp. 410–414.

[10] I. Diahovchenko, M. Kolcun, Z. Čonka, 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. 1319–1333, Dec. 2020.

[11] M. Jaganmohan. (Mar. 3, 2022). Global Smart Grid Market Size by Region 2017–2023. [Online]. Available: https://www.statista.com/statistics/246154/global-smart-grid-marketsize-by-region/

[12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou. (Sep. 30, 2021). Electricity Theft Detection, [Online]. Available: https://github.com/henryRDlab/ ElectricityTheftDetection

[13] 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. 59–69, 2015.

[14] 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. 1–8, 2017.