A

Major Project

On

# ELECTRICITY THEFT DETECTION IN SMART GRIDS BASED ON DEEP NEURAL NETWORK

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

K.HARSHITHA(207R1A0587)

P.KARTHIK(207R1A05B0)

MOHAMMED MOKHIM(207R1A0598)

Under the Guidance of

**A.UDAY KIRAN**

(Assistant Professor)


**DEPARTMENT OF COMPUTER SCIENCEAND ENGINEERING**

**CMR TECHNICALCAMPUS**

**UGC AUTONOMOUS**

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, NewDelhi) Recognized Under Section 2(f) & 12(B) of the UGCAct.1956, Kandlakoya (V), Medchal Road, Hyderabad-501401.

**2020-2024**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**


# CERTIFICATE

This is to certify that the project entitled "**ELECTRICITY THEFT DETECTION IN SMART GRIDS BASED ON DEEP NEURAL NETWORK**" being submitted by **Kotagiri Harshitha (207R1A0587), Peddagolla Karthik (207R1A05B0)** and **Mohammed Mokhim (207R1A0598)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of bonafide work carried out by them under our guidance and supervision during the year 2023-24.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

**A.Uday Kiran**
(Assistant Professor)
INTERNAL GUIDE

**Dr. A. Raji Reddy**
DIRECTOR

**Dr. K. Srujan Raju**
HOD

**EXTERNAL EXAMINER**

**Submitted for viva voice Examination held on _____**

# ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express our profound gratitude and deep regard to our guide **A. Uday Kiran,** Assistant Professor for his exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) **Dr. J. Narasimharao, G.Vinesh Shanker, Ms. Shilpa, & Dr. K. Maheswari** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Srujan Raju,** Head, Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We also express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

**K. HARSHITHA (207R1A0587)**

**P. KARTHIK (207R1A05B0)**

**MD. MOKHIM (207R1A0598)**

# ABSTRACT

Electricity theft is a global problem that negatively affects both utility companies and electricity users. It destabilizes the economic development of utility companies, causes electric hazards and impacts the high cost of energy for users. The development of smart grids plays an important role in electricity theft detection since they generate massive data that includes customer consumption data which, through machine learning and deep learning techniques, can be utilized to detect electricity theft. This paper introduces the theft detection method which uses comprehensive features in time and frequency domains in a deep neural network-based classification approach.

We address dataset weaknesses such as missing data and class imbalance problems through data interpolation and synthetic data generation processes. We analyze and compare the contribution of features from both time and frequency domains, run experiments in combined and reduced feature space using principal component analysis and finally incorporate minimum redundancy maximum relevance scheme for validating the most important features. Lastly, we show the competitiveness of our method in comparison with other methods evaluated on the same dataset. On validation, we obtained 97% area under the curve (AUC), which is 1% higher than the best AUC in existing works, and 91.8% accuracy, which is the second-best on the benchmark.

# LIST OF FIGURES/TABLES

# LIST OF SCREENSHOTS

# TABLE OF CONTENTS

# 1. INTRODUCTION

# 1. INTRODUCTION

## 1.1 PROJECT SCOPE

The project on "Electricity Theft Detection in Smart Grids based on deep neural network" aims to address a critical challenge in the field of energy distribution and management. As smart grids become increasingly prevalent, the need for robust security measures to detect and prevent electricity theft becomes paramount. The project scope involves the development and implementation of a sophisticated deep neural network (DNN) system designed to analyze and interpret data from smart grid sensors. This DNN will be trained to recognize patterns and anomalies in electricity consumption that may indicate unauthorized access or tampering. By addressing electricity theft, the project contributes to the overall reliability, efficiency, and security of smart grids, fostering a more sustainable and resilient energy infrastructure.

## 1.2 PROJECT PURPOSE

The purpose of the project is to enhance the security and integrity of smart grids by developing an effective electricity theft detection system based on deep neural networks. Electricity theft poses a significant challenge to utility providers, leading to revenue losses, increased operational costs, and potential safety hazards. The project seeks to mitigate these issues by leveraging advanced machine learning techniques to create a robust and adaptive system.

## 1.3 PROJECT FEATURES

The proposed project on "Electricity Theft Detection in Smart Grids based on deep neural network" encompasses a comprehensive set of features to fortify the security and efficiency of modern energy distribution systems.The DNN will be trained to detect anomalies indicative of electricity theft, ensuring adaptability to evolving tactics through continuous learning mechanisms. Real-time monitoring capabilities will be integrated, allowing for instantaneous alerts and timely responses to suspicious activities. The system will feature a user-friendly interface for utility operators, complete with detailed reports and visualizations. Seamless integration with existing smart grid infrastructure, scalability, and robust security measures against adversarial attacks will be paramount considerations. By incorporating these features, the project aims to deliver a cutting-edge solution that enhances the reliability, security, and sustainability of smart grids.

# 2. LITERATURE SURVEY

# 2. LITERATURE SURVEY

**Damian O. Dike Uchechukwu A. Obiora1, Euphemia C. Nwokorie, Blessing C. Dike 2015:** The design, simulation and construction of a GSM-based prepaid meter has been achieved. It x-rayed various forms of electricity theft which include unaccountability of servicemen, irregularities of billing leading to a reduction of funds by the utility companies has also been achieved as this work prevents one on one contact between the end user and the workers. With remote monitoring of the meter reading and sending SMS whenever there is readings in the customer electricity meter, the developed system may be able to help Utilities reduce the incidences of household electricity theft. The work also revolves around the automatic disconnection and connection when the recharge is low or high respectively and extra cost due to reconnection is removed. Further improvement will be needed in including miniaturized monitoring cameras in the customer meter which will monitor physical activities around the meter in each household to check other illegal acts that were not covered in this work.

**Zibin Zheng,Yatao Yang, Xiangdong Niu, Hong-Ning Dai, Yuren Zhou 2017:** They propose a Wide & Deep CNN model to detect electricity theft in smart grids. In particular, our Wide & Deep CNN model consists of the Wide component and the Deep CNN component; it gains the benefits of memorization and generalization brought by the Wide component and the Deep CNN component, respectively. We conduct extensive experiments on realistic electricity consumption data released by State Grid Corporation of China (SGCC), the largest electricity supply company in China. The experiment results show that our proposed Wide & Deep CNN outperforms existing methods, such as linear regression, support vector machine. Since it consumes extremely high amounts of electricity to grow marihuana, the abnormal electricity usage patterns can be captured by the proposed wide and deep CNN model.

**Mubbashra Anwar,Nadeem Javaid, Adia Khalid, Muhammad Imran, Muhammad Shoaib 2020:** In this work, a pipeline is proposed to detect electricity

theft in SG. The proposed pipeline is made up of SMOTE,KPCA and SVM. The imbalanced class issue is resolved using SMOTE, KPCA is used for feature extraction and SVM for the classification of electricity theft. It is the most efficient and simplest technique that is able to classify the fraudulent and non-fraudulent consumers accurately. Besides, various performance metrics are used for the evaluation of binary classification problems, such as: ROC curve, precision, recall, F1-score, MCC, and MAP are used to evaluate the performance of the proposed model. The proposed method is general and can be applied to any field to detect the anomaly. However, our contribution is just a small step towards the goal of accurate detection of NTLs. In future, the generative adversarial networks (GANs) will be explored to tackle the issue of class imbalance by generating more realistic data for minority class and also for the anomaly detection task.

# 3. SYSTEM ANALYSIS

# 3. SYSTEM ANALYSIS

## 3. SYSTEM ANALYSIS

System Analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important role of an interrogator and dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done. A key question considered here is, “what must be done to solve the problem?” The system is viewed as a whole and the inputs to the system are identified.

Once analysis is completed the analyst has a firm understanding of what is to be done.

## 3.1 PROBLEM DEFINITION

The “Electricity Theft Detection in Smart Grids based on deep neural network” project is motivated by the pressing issue of unauthorized electricity consumption, commonly referred to as electricity theft, within smart grid infrastructures. This problem poses significant challenges for utility providers, leading to financial losses, increased operational costs, and potential safety hazards. Current methods for detecting electricity theft often lack the precision and adaptability needed to address evolving strategies employed by offenders. Consequently, there is a critical need for an advanced system that leverages deep neural networks to analyze real-time data from smart grid sensors, identify anomalies in electricity consumption patterns, and provide timely alerts to utility operators. By addressing this problem, the project aims to enhance the overall security, efficiency, and sustainability of smart grids.

## 3.2 EXISTING SYSTEM

Hardware-based method, generally require hardware devices such as specialized microcontrollers, sensors and circuits to be installed on power distribution lines. These methods are generally designed to detect electricity theft done by physically tampering with distribution components such as distribution lines and electricity meters. They can not detect cyber attacks. Electricity cyber attack is a form of electricity theft whereby energy consumption data is modified by hacking the electricity meters. For instance, an electricity meter was re-designed. It used components that include: a Global System for Mobile Communications (GSM) module, a microcontroller, and an Electrically Erasable Programmable Read-Only Memory (EEPROM). A simulation was done and the meter was able to send a Short Message Service (SMS) whenever an illegal load was connected by bypassing the meter. Limited to detecting electricity theft done by physically tampering with distribution components such as distribution lines and electricity meters. Authors in used the GSM module, ARM-cortex M3 processor and other hardware components to solve the electricity theft problem done in the following four ways: bypassing the phase line, bypassing the meter, disconnecting the neutral line, and tampering with the meter to make unauthorized modifications. A prototype was built to test all four possibilities. The GSM module was able to notify with SMS for each theft case.

### 3.2.1 LIMITATIONS OF EXISTING SYSTEM

Following are the disadvantages of existing system:

- An existing system not implemented dnn-based electricity theftdetection method.
- An existing system not implemented Hyperbolic tangent activation function.

## 3.3 PROPOSED SYSTEM

Based on the literature, we propose a novel DNN classification-based electricity theft detection method using comprehensive time-domain features. We further propose using frequency-domain features to enhance performance. We employ Principal Component Analysis (PCA) to perform classification with reduced feature space and compare the results with classification done with all input features to interpret the results and simplify the future training process.We further use the Minimum Redundancy Maximum Relevance (mRMR) scheme to identify the most significant features and validate the importance of frequency-domain features over time-domain features for detecting electricity theft.

We optimize the hyperparameters of the model for overall improved performance using a Bayesian optimizer. We further employ an adaptive momentestimation(Adam) optimizer to determine the best ranges of values of the other keyparameters that can be used to achieve good results with optimal model trainingspeed.Lastly, we show 1% improvement in AUC and competitive accuracy of ourmodel in comparison to other data-driven electricity theft detection methods in the literature evaluated on the same dataset.

### 3.3.1 ADVANTAGES OF THE PROPOSED SYSTEM

Huge amount of data obtained by cloud providers and other businesses, making large datasets that train DNNs effectively.

Advances in machine learning and signal/information processing research which leads to the evolution of techniques to improve accuracy and broaden the domain of DNNs application.

## 3.4 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and a business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. Three key considerations involved in the feasibility analysis:

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

### 3.4.1 ECONOMIC FEASIBILITY

The developing system must be justified by cost and benefit. Criteria to ensure that effort is concentrated on a project, which will give best, return at the earliest. One of the factors, which affect the development of a new system, is the cost it would require. The following are some of the important financial questions asked during preliminary investigation:

- The cost of the hardware and software.
- The benefits in the form of reduced costs or fewer costly errors.

Since the system is developed as part of project work, there is no manual cost to spend for the proposed system. Also all the resources are already available, it give an indication that the system is economically possible for development.

### 3.4.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

### 3.4.3 SOCIAL FEASIBILITY

The social feasibility of implementing a malicious URL detection system based on machine learning involves evaluating its acceptance and impact within the user and broader societal context. A critical consideration is the level of trust users place in the system's ability to accurately identify malicious URLs without compromising user privacy. Transparency in the decision-making process of the machine learning model is essential to foster understanding and confidence among users.

## 3.5 HARDWARE & SOFTWARE REQUIREMENTS

### 3.5.1 HARDWARE REQUIREMENTS:

Hardware interfaces specify the logical characteristics of each interface between the software product and the hardware components of the system. The following are some hardware requirements.

- Processor : Pentium –IV
- RAM : 4 GB (min)
- Hard Disk : 20 GB
- Key Board : Standard Windows Keyboard
- Mouse : Two or Three Button Mouse
- Monitor : SVGA

### 3.5.2 SOFTWARE REQUIREMENTS:

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements.

- Operating system : Windows 7 Ultimate.
- Coding Language : Python.
- Front-End : HTML.
- Back-End : Django-ORM
- Designing : Html, css, javascript.
- Data Base : MySQL (WAMP Server).

# 4. ARCHITECTURE

# 4. ARCHITECTURE

## 4.1 PROJECT ARCHITECTURE

This project architecture shows the procedure followed for classification, starting from input to final prediction.

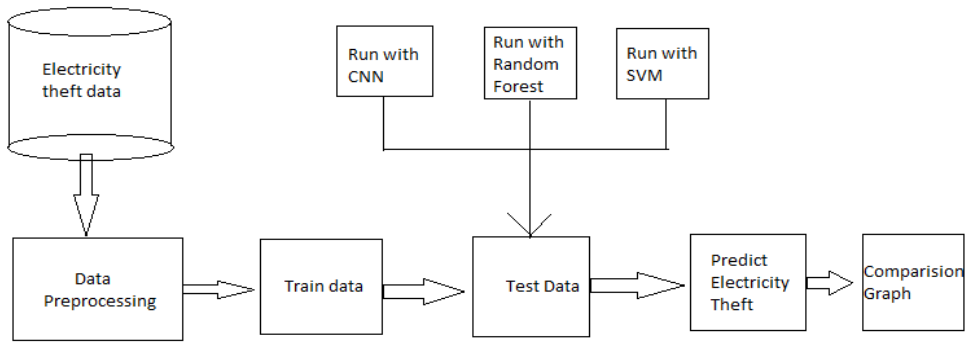



Figure 4.1: Project Architecture for Electricity Theft Detection in smart grids based on deep neural network

## 4.2 DESCRIPTION

The "Electricity Theft Detection in Smart Grids based on deep neural network" project aims to enhance the security of modern energy distribution systems. Using a carefully designed deep neural network, the system analyzes real-time data from smart grid sensors to detect anomalies in electricity consumption patterns that may indicate theft. The architecture incorporates continuous learning mechanisms, ensuring adaptability to evolving theft strategies. With a user-friendly interface for operators and seamless integration with existing infrastructure, the project seeks to provide a comprehensive solution for prompt and effective theft detection, contributing to the overall reliability and security of smart grids.

## 4.3 USE CASE DIAGRAM

In the use case diagram, we have basically two actors one is the remote user and other is the service provider.

A use case diagram is a graphical depiction of a user's possible interactions with a system. The use cases are represented by either circles or ellipses. The actors are often shown as stick figures.

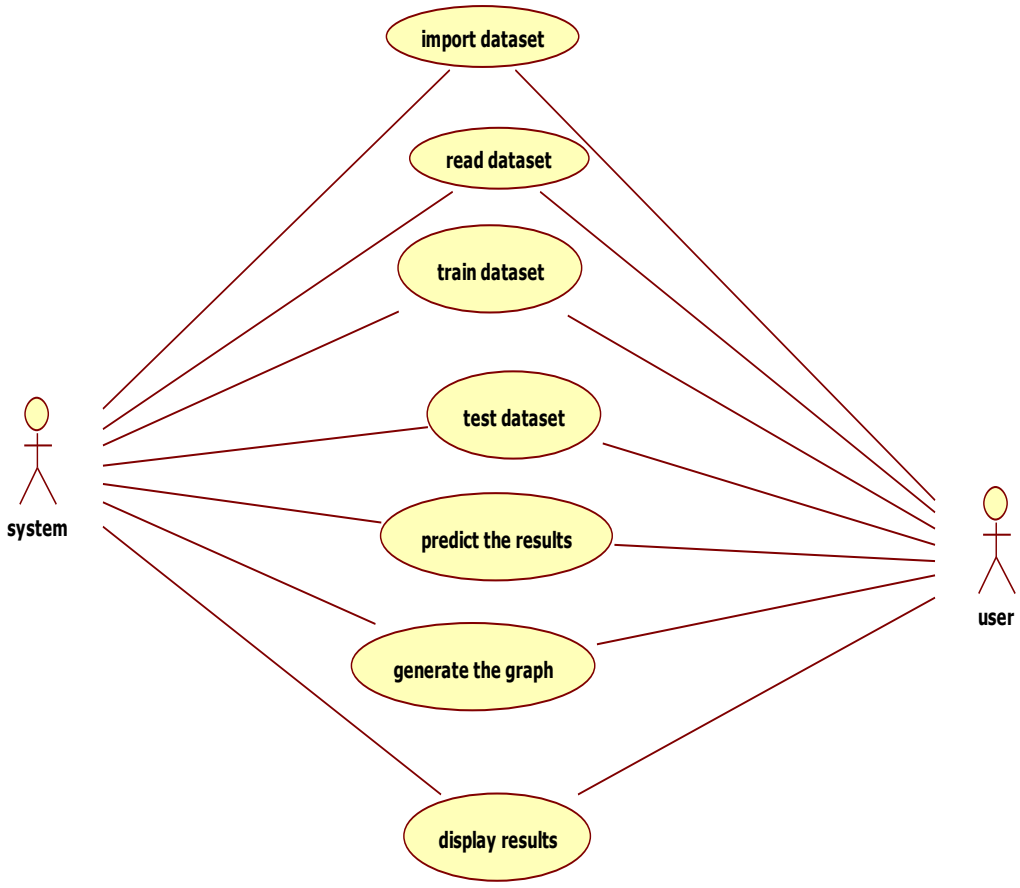



Figure 4.2: Use Case Diagram for Electricity Theft Detection in Smart grids based on deep neural network

## 4.4 CLASS DIAGRAM

Class diagram is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations(or methods), and the relationships among objects.

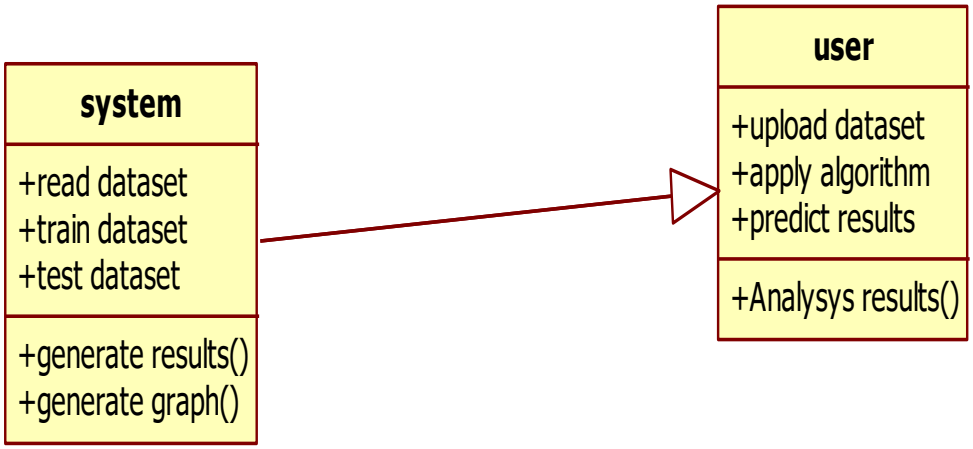



Figure 4.3: Class Diagram for Electricity Theft Detection in Smart grids based on deep neural network

## 4.5 SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the logical view of the system under development.

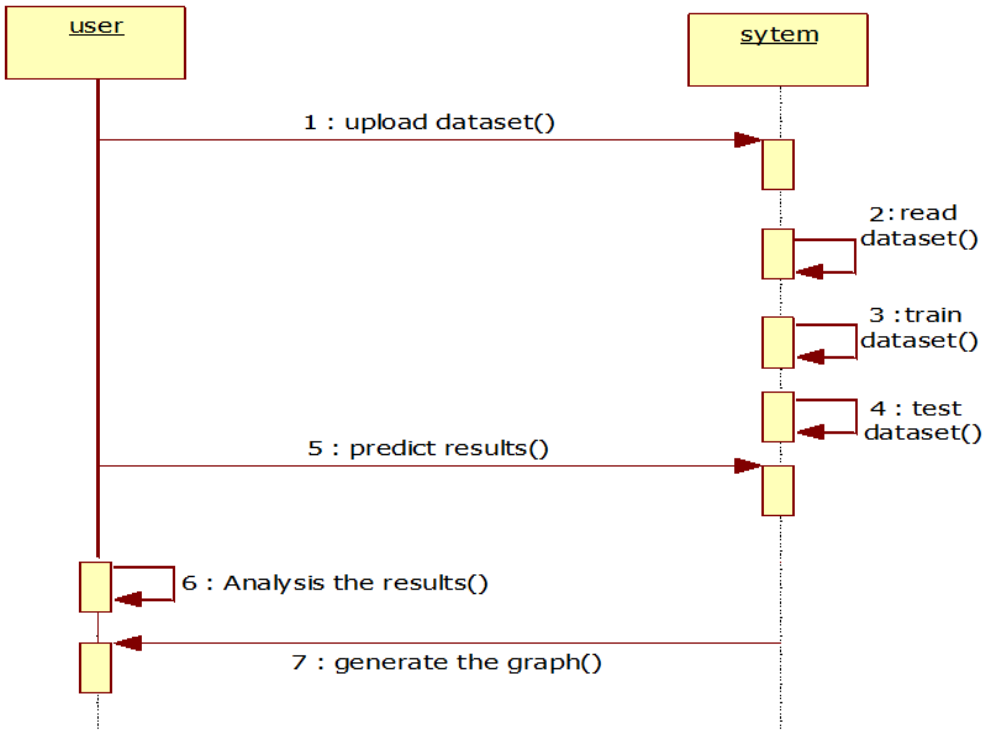



Figure 4.4: Sequence Diagram for Electricity Theft Detection in Smart grids based on deep neural network

## 4.6 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. They can also include elements showing the flow of data between activities through one or more data stores.

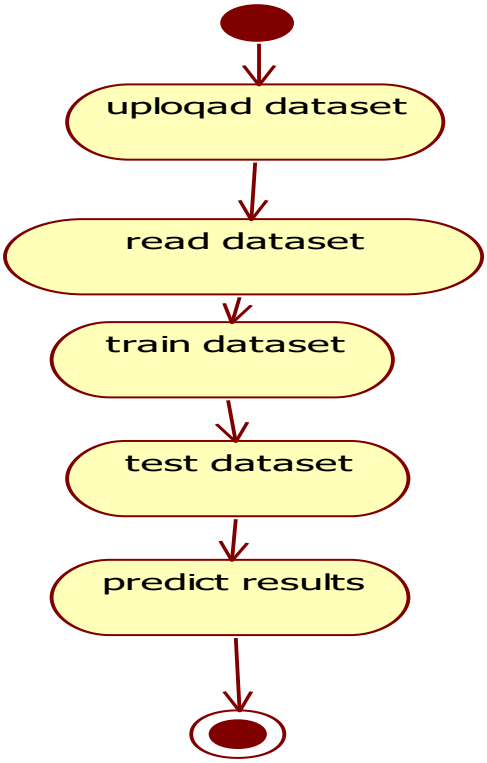



Figure 4.5: Activity Diagram for Electricity Theft Detection in Smart grids based on deep neural network

# 5. IMPLEMENTATION

## 5.1 SAMPLE CODE

```
from tkinter import *
import tkinter
from tkinter import filedialog
import numpy as np
from tkinter.filedialog import askopenfilename
import pandas as pd
from tkinter import simpledialog
import pandas as pd
import numpy as np
from sklearn.preprocessing import LabelEncoder
from sklearn.preprocessing import normalize
from keras.models import Sequential, Model
from keras.layers import Dense, Dropout, Activation
from keras.utils.np_utils import to_categorical
from keras.models import model_from_json
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import precision_score
from sklearn.metrics import recall_score
from sklearn.metrics import f1_score
from sklearn.metrics import accuracy_score
from sklearn.model_selection import train_test_split
from sklearn import svm
import os
```

```
import matplotlib.pyplot as plt

main = tkinter.Tk()

main.title("Electricity Theft Detection in Smart Grids based on Deep Neural Network")

main.geometry("1000x650")

global filename

global cnn_model

global X, Y

global le

global dataset

accuracy = []

precision = []

recall = []

fscore = []

global classifier

def uploadDataset():

    global filename

    global dataset

    filename = filedialog.askopenfilename(initialdir = "Dataset")

    text.delete('1.0', END)

    text.insert(END,filename+' Loaded\n')

    dataset = pd.read_csv(filename)

    text.insert(END,str(dataset.head())+"\n\n")

def preprocessDataset():
```

```
    global dataset
    le = LabelEncoder()
    text.delete('1.0', END)
    dataset.fillna(0, inplace = True)
    dataset['client_id'] = pd.Series(le.fit_transform(dataset['client_id'].astype(str)))
    dataset['label'] = dataset['label'].astype('uint8')
    print(dataset.info())
    dataset.drop(['creation_date'], axis = 1,inplace=True)
    text.insert(END,str(dataset.head())+"\n\n")
    dataset = dataset.values
    X = dataset[:,0:dataset.shape[1]-1]
    Y = dataset[:,dataset.shape[1]-1]
    Y = Y.astype('uint8')
    indices = np.arange(X.shape[0])
    np.random.shuffle(indices)
    X = X[indices]
    Y = Y[indices]
    Y = Y.astype('uint8')
    text.insert(END,"Total records found in dataset to train Deep Learning :
"+str(X.shape[0])+"\n\n")
    def runCNN():
    global X, Y
    text.delete('1.0', END)
```

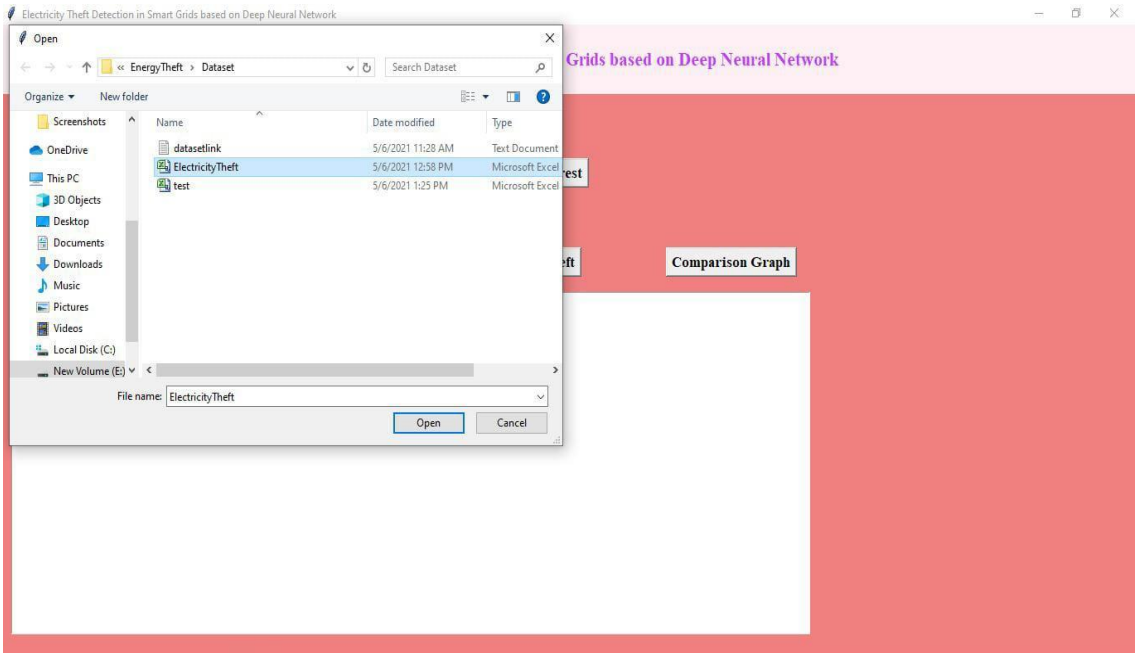
```
global cnn_model
    accuracy.clear()
    precision.clear()
    recall.clear()
     Y1 = to_categorical(Y)
    Y1 = Y1.astype('uint8')
    if os.path.exists('model/model.json'):
        with open('model/model.json', "r") as json_file:
            loaded_model_json = json_file.read()
            cnn_model = model_from_json(loaded_model_json)
        json_file.close()
        cnn_model.load_weights("model/model_weights.h5")
        cnn_model._make_predict_function()
        print(cnn_model.summary())
    else:
        counts = np.bincount(Y1[:, 0])
        weight_for_0 = 1.0 / counts[0]
        weight_for_1 = 1.0 / counts[1]
    text.insert(END,"CNN Accuracy  : "+str(f)+"\n\n")
def runCNNRF():
    recall.append(r)
    fscore.append(f)
    text.insert(END,"CNN with Random Forest Precision : "+str(p)+"\n")
    text.insert(END,"Random Forest Precision : "+str(p)+"\n")
```

```
cnnrfButton = Button(main, text="CNN with Random Forest",
command=runCNNRF)

cnnrfButton.place(x=500,y=150)

cnnrfButton.config(font=font1)

cnnsvmButton = Button(main, text="CNN with SVM", command=runCNNSVM)

cnnsvmButton.place(x=200,y=200)

cnnsvmButton.config(font=font1)

rfButton = Button(main, text="Run Random Forest", command=runRandomForest)

rfButton.place(x=500,y=200)

svmButton = Button(main, text="Run SVM Algorithm", command=runSVM)

svmButton.place(x=200,y=250)

svmButton.config(font=font1)

predictButton = Button(main, text="Predict Electricity Theft", command=predict)

predictButton.place(x=500,y=250)

predictButton.config(font=font1)

graphButton = Button(main, text="Comparison Graph", command=graph)

graphButton.place(x=800,y=250)

graphButton.config(font=font1)

font1 = ('times', 12, 'bold')

text=Text(main,height=20,width=120)

text.configure(yscrollcommand=scroll.set)

text.place(x=10,y=300)

text.config(font=font1)

main.config(bg='light coral')
```

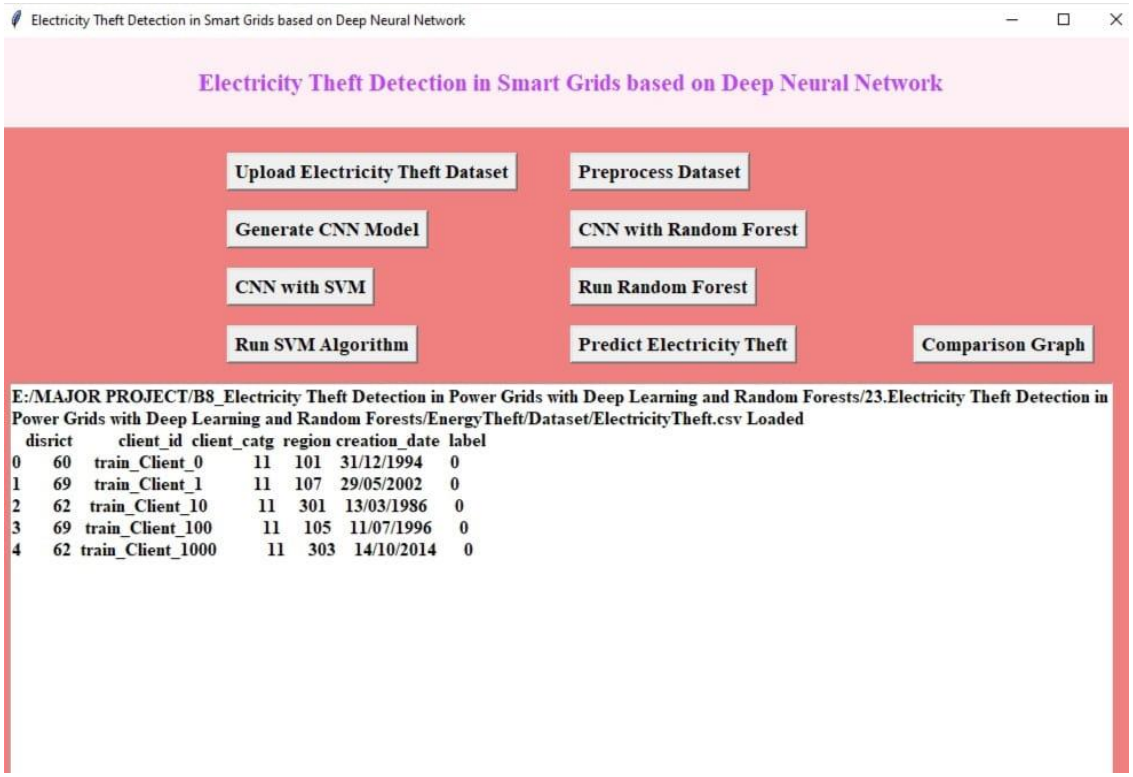
# 6. SCREENSHOTS


.

Screenshot 6.1 Interface of the project

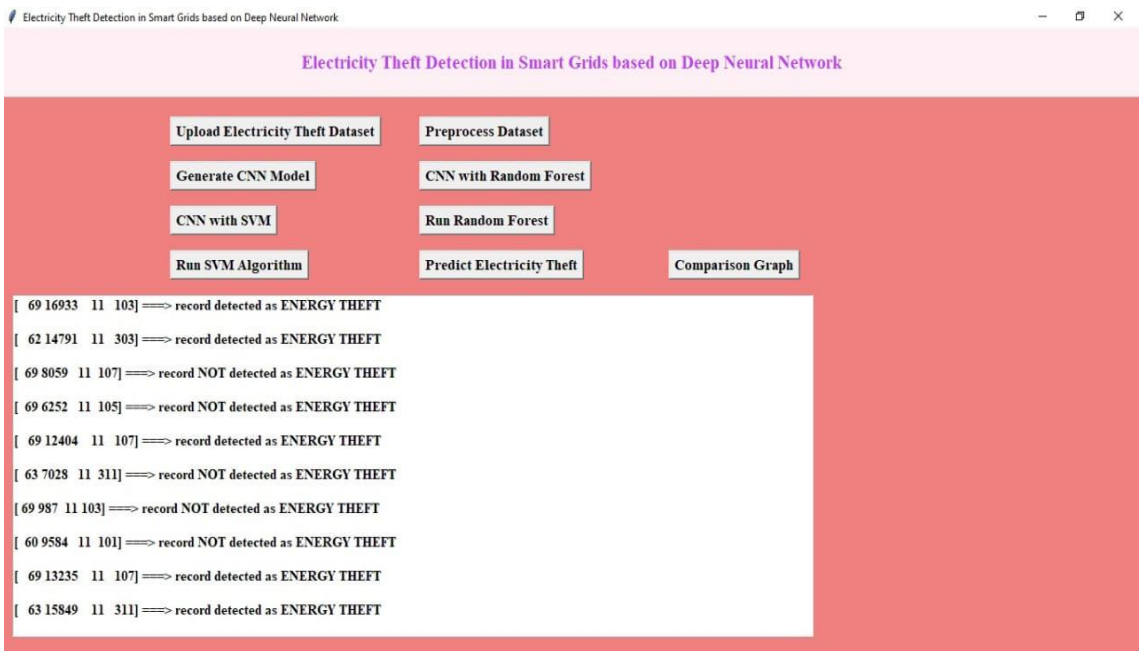



Screenshot 6.2 Upload Dataset

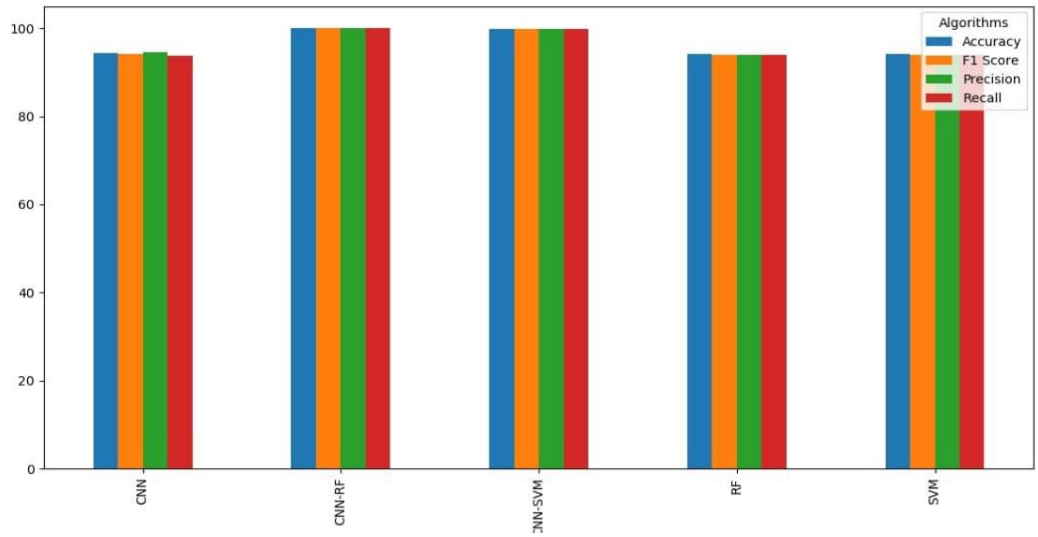



Screenshot 6.3 Training the dataset


Screenshot 6.4 Testing with various algorithms




Screenshot 6.5 Prediction of Electricity Theft




Screenshot 6.6 Comparision Graph

# 7. TESTING

# 7. TESTING

## 7.1 INTRODUCTION TO TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

## 7.2 TYPES OF TESTING

### 7.2.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .It is done after the completion of an individual unit before integration. This is a structural testing that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

### 7.2.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Integration tests demonstrate that

although the components were individually satisfactory, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

### 7.2.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid : identified classes of invalid input must Input be rejected

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked. Organization and preparation of functional tests is focused on requirements, key functions, or special test cases.

## 7.3 TEST CASES

### 7.3.1 CLASSIFICATION

| Test case ID | Test case name | Purpose | Input | Output |
|---|---|---|---|---|
| 1 | Remote user Uploads tweet datasets | It predicts the theft done or not | The remote user uploads the dataset | By using algorithms it predicts the electricity theft |
| 2 | Predict the electricity theft | It is used to predict the electricity theft | The remote user uploads the dataset | It predicts whether the theft is happened or not |
| 3 | Train and test datasets | It is used to predict how much theft is done | Uploads the dataset | It displays the comparision graph. |

# 8. CONCLUSION

# 8. CONCLUSION & FUTURE SCOPE

## 8.1 CONCLUSION

In conclusion, the application of deep neural networks for electricity theft detection in smart grids represents a promising and effective approach. This technology has the potential to revolutionize the way utilities and grid operators identify and mitigate unauthorized consumption, ultimately improving the reliability and sustainability of our energy infrastructure. By analyzing vast amounts of data from smart meters and other grid sensors, deep neural networks can accurately pinpoint irregularities and anomalies in power consumption patterns, facilitating early detection of electricity theft.The advantages include their ability to adapt to complex and evolving patterns of theft, their high accuracy rates, and their potential for real-time monitoring and response. Additionally, they can reduce operational costs and revenue losses for utilities, benefiting both providers and consume.

## 8.2 FUTURE SCOPE

In the future, a project on detecting electricity theft in smart grids using deep neural networks could grow in several ways. Firstly, the accuracy of the detection system could be improved by using more advanced algorithms and tweaking the settings to make it more precise. Secondly, the system could be made faster to detect theft as it happens, by optimizing how it processes data from smart meters and other sensors. Thirdly, it could be expanded to look for unusual patterns in electricity use that might suggest theft, even in cases where traditional methods might not spot it. Fourthly, the system could be made to work efficiently in very large smart grid networks with millions of users. Additionally, it could be integrated more closely with other parts of the smart grid, like smart meters and control systems, to make monitoring and control easier.

# 9. BIBLIOGRAPHY

# 9. BIBILIOGRAPHY

## 9.1 REFERENCES


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


## 9.2 GITHUB LINK

https://github.com/Harshitha-31/Electricity-theft-detection-in-smart-grids-based-on-deep-neural-network