Detection of Electricity Theft In Smart Meter Using Convolutional Neural Network

A.Anifer [1],D.Siva Senthil[2]
[1, 2] Dept of CSE
[1, 2] Arunachala College Of Engineering

Abstract*- Energy theft constitutes a major concern for the utility operators in these modern smart homes. The task of detecting and reducing the energy losses has been highly challenging due to insufficient inspection techniques. Energy distribution is comprised of Technical and Non-Technical Losses (NTL). Energy theft generates a major share of Non-Technical Losses which also prompts budgetary misfortunes for the service organizations. The data in the modern smart meters are transmitted in wireless mode. Therefore the smart homes are vulnerable to energy theft. Many new technologies have been adopted to resolve the issue of energy theft in Advance Metering Infrastructure (AMI) in Smart Grids. Consumption pattern must be derived to identify illegal energy consumers. Computational method has been derived to analyze and identify energy consumption patterns based on data mining techniques. Machine learning technique improves the got client energy utilization readings and guides them on contrasting irregularities in use. Deep Learning method as Convolution Neural Network is implemented on the activity of order methods on client energy utilization and illegal use of electricity and the amount of consumption by energy theft. The data in the modern smart meters are transmitted in wireless mode. Therefore the smart homes are vulnerable to energy theft. CNN2D model is used to identify electricity theft in smart grids. In particular, a deep learning model is used for electricity theft detection which is based on convolutional neural network. The main advantage of using CNN2D is that these neural networks extract all the important features of the data without any human supervision.*

Keywords*-* Energy distribution, Non-Technical Losses,Advance Metering Infrastructure, Deep Learning, Convolution Neural Network, CNN2D.

I. INTRODUCTION

IoT was generally defined as dynamic global network infrastructure with self configuring capabilities based on standards and interoperable communication protocols; physical and virtual ‘things’ in an IoT have identities and attributes and are capable of using intelligent interfaces and being integrated as an information network. The purpose of IoT is to increase the functions of the first version of Internet and make it more useful. With IoT, users can share both information provided by humans that contained in databases and also information provided by things in physical world. Describe the IoT as the connection of physical things to the Internet and to each other for various useful purposes through different intelligent technologies, creating smart ecosystem of pervasive computing. It can also be described as including embedded intelligence in individual objects that can notice changes in their physical state. The common definition of IoT is that computers, sensors, and objects interact with each other and process data, therefore IoT is a new technology system combined of a number of information technologies. The IoT combines different technologies into a semi-autonomous network. It connects individual devices to the network and to each other.

Smart environments are aimed to exploit rich combinations of small computational nodes to identify and deliver personalized services to the user while interact and exchange information with the environment. IoTs technology can be applied to create smart homes in order to provide intelligence, comfort and to improve the quality of lives. A “smart home” can be defined as a home which is automated through the application of the Internet of Things technologies and capable of reacting to requirements of the inhabitants, providing comfort, security, safety and entertainment.

The most common and simplest way of pilfering electricity is tapping energy directly from an overhead distribution feeder. The next most prominent method of electricity theft is the manipulation of energy meters that are used for recording and billing industrial, commercial and household energy consumption. In the case of electronic meters, Radio Frequency (RF) devices are mounted to In general, illegal consumption of electricity will be predominant only at desired hours of the day - when the customer’s demand is high i.e. using legal electricity for small household loads and illegally tapped electricity for heavy loads. This kind of theft (partial illegal consumption) is very difficult to measure, as the energy consumption pattern is uneven over a period of time. In addition, corrupt employees are often responsible for billing irregularities; record an amount of consumption that is lower than the original consumption.

Factors that influence consumers to steal electricity depend upon various local parameters that fall into multiple categories like social, political, economic, literacy, law, managerial, infrastructural, and economical. Of these factors, socio-economic factors influence people to a greater extent in stealing electricity. More concisely, some of the important factors are:

- The belief that it is dishonest to steal something from a neighbor but not from a utility (public or large entity).
- Higher energy prices, unemployment or weak economic situation of a consumer.
- Corrupt politicians and employees of the utilities are responsible for billing irregularities.
- In some cases, total money spent on bribing utility employees is less than the money that would have been paid for consuming the same amount of electricity legally.
- Some consumers might not be literate about the issues, laws and offenses related to the energy theft.
- Weak accountability and enforcement of law.
- Reasons to hide total energy consumption (e.g. Consumers who grow marijuana illegally or small-scale industries to hide overall production/turnover).
- The smart meter data is collected and preprocess the raw data of records to remove irrelevant factors.
- The machine learning algorithms are used to analyze the data that literally cluster and then classify the Customer. The trustworthiness of customers is find by using PCA.
- Mean Shift clustering algorithm is applied to detect anomalies and irregularities in the collected data by clustering.
- The customer’s data are discriminated as genuine and fraud based on their usage pattern.
- CNN is applied to classify the user profile with more accuracy.
- CNN is trained with all subsets to detect the energy theft and validation is performed on the testing subsets.

II. LITERATURE SURVEY

The two-way flow of information and energy is an important feature of the Energy Internet. Data analytics is a powerful tool in the information flow that aims to solve practical problems using data mining techniques. As the problem of electricity thefts via tampering with smart meters continues to increase, the abnormal behaviors of thefts become more diversified and more difficult to detect. Thus, a data analytics method for detecting various types of electricity thefts is required. However, the existing methods either require a labeled dataset or additional system information which is difficult to obtain in reality or have poor detection accuracy. In this paper, combine two novel data mining techniques to solve the problem. One technique is the Maximum Information Coefficient (MIC), which can find the correlations between the non-technical loss (NTL) and a certain electricity behavior of the consumer. MIC can be used to precisely detect thefts that appear normal in shapes. The other technique is the clustering technique by fast search and find of density peaks (CFSFDP). CFSFDP finds the abnormal users among thousands of load profiles, making it quite suitable for detecting electricity thefts with arbitrary shapes. Next, a framework for combining the advantages of the two techniques is proposed. Numerical experiments on the Irish smart meter dataset are conducted to show the good performance of the combined method.

The widespread deployment of Automatic Metering Infrastructures in Smart Grid scenarios rises great concerns about privacy preservation of user-related data, from which detailed information about customer’s habits and behaviors can be deduced. Therefore, the users’ individual measurements should be aggregated before being provided to External Entities such as utilities, grid managers and third parties. This paper proposes a security architecture for distributed aggregation of additive data, in particular energy consumption metering data, relying on Gateways placed at the customers’ premises, which collect the data generated by local Meters and provide communication and cryptographic capabilities. The Gateways communicate with one another and with the External Entities by means of a public data network. We propose a secure communication protocol aimed at preventing Gateways and External Entities from inferring information about individual data, in which privacy-preserving aggregation is performed by means of a cryptographic homomorphic scheme. The routing of information flows can be centralized or it can be performed in a distributed fashion using a protocol inspired by Chord. Compare the performance of both approaches to the optimal solution minimizing the data aggregation delay.

Energy theft constitutes an issue of great importance for electricity operators. The attempt to detect and reduce non-technical losses is a challenging task due to insufficient inspection methods. With the evolution of advanced metering infrastructure (AMI) in smart grids, a more complicated status quo in energy theft has emerged and many new technologies are being adopted to solve the problem. In order to identify illegal residential consumers, a computational method of analyzing and identifying electricity consumption patterns of consumers based on data mining techniques has been presented. Combining principal component analysis (PCA) with mean shift algorithm for different power theft scenarios, we can now cope with the power theft detection problem sufficiently. The overall research has shown encouraging results in residential consumers power theft detection that will help utilities to improve the reliability, security and operation of power network.

For the smart grid energy theft identification, this letter introduces a gradient boosting theft detector (GBTD) based on the three latest gradient boosting classifiers (GBCs): 1) extreme gradient boosting; 2) categorical boosting; and 3) light gradient boosting method. While most of existing machine learning (ML) algorithms just focus on fine tuning the hyper parameters of the classifiers, our ML algorithm, GBTD, focuses on the feature engineering-based preprocessing to improve detection performance as well as time-complexity. GBTD improves both detection rate and false positive rate (FPR) of those GBCs by generating stochastic features like standard deviation, mean, minimum, and maximum value of daily electricity usage. GBTD also reduces the classifier complexity with weighted feature importance-based extraction techniques. Emphasis has been laid upon the practical application of the proposed ML for theft detection by minimizing FPR and reducing data storage space and improving time-complexity of the GBTD classifiers. Additionally, this letter proposes an updated version of the existing six theft cases to mimic real-world theft patterns and applies them to the dataset for numerical evaluation of the proposed algorithm.

Electricity theft is a widespread problem that causes tremendous economic losses for all utility companies around the globe. As many countries struggle to update their antique power systems to emerging smart grids, more and more smart meters are deployed throughout the world. Compared with analog meters which can be tampered with by only physical attacks, smart meters can be manipulated by malicious users with both physical and cyber-attacks for the purpose of stealing electricity. Thus, electricity theft will become even more serious in a smart grid than in a traditional power system if utility companies do not implement efficient solutions. The goal of this paper is to identify all malicious users in a neighborhood area in a smart grid within the shortest detection time. We propose an adaptive binary splitting inspection (ABSI) algorithm which adopts a group testing method to locate the malicious users. There are two considered inspection strategies in this paper: a scanning method in which users will be inspected individually, and a binary search method by which a specific number of users will be examined as a whole. During the inspection process of our proposed scheme, the inspection strategy as well as the number of users in the groups to be inspected are adaptively adjusted. Simulation results show that the proposed ABSI algorithm outperforms existing methods.

Distribution of electricity involves both technical losses and NTL. NTL accounts for up to 10–40% of total energy distributed. A major portion of NTL is due to electricity theft. Transmission and distribution of electricity involve technical as well as Non-Technical Losses (NTLs). Electricity theft includes tapping energy directly from the distribution feeder, tampering with the energy meter, or using physical methods to evade payment. Improper calibration and illegal de-calibration of energy meters during their design can also cause NTL. Several engineered methods are also implemented to manipulate the energy consumption measured by the energy meter. Illegal consumers may use legal electricity from the energy meter for smaller household loads and illegally tapped electricity for heavier loads. Illegal consumption of electricity constitutes a major portion of the NTL at distribution feeder level. Considering the severity and devastating effects of the problem, illegal consumption of electricity has to be detected instantly in real-time. To this end, this paper investigates the possibility and role of High Performance Computing (HPC) algorithms in detection of illegal consumers. This paper designs and implements an encoding procedure to simplify and modify customer energy consumption data for quicker analysis without compromising the quality or uniqueness of the data.

Large scale consumption of electricity in a fraudulent manner may imbalance the demand-supply gap to a great extent. Thus, there arises the need to develop a scheme which can detect these thefts precisely in the complex power networks. So, keeping focus on these points, this paper proposes a comprehensive top-down scheme based on decision tree (DT) and support vector machine (SVM). Unlike existing schemes, the proposed scheme is capable enough to precisely detect and locate real-time electricity theft at every level in power transmission and distribution. The proposed scheme is based on the combination of DT and SVM classifiers for rigorous analysis of gathered electricity consumption data. In other words, the proposed scheme can be viewed as a two level data processing and analysis approach, since the data processed by DT is fed as an input to the SVM classifier. Furthermore, the obtained results indicate that the proposed scheme reduces false positives to a great extent and is practical enough to be implemented in real-time scenarios. It parallelizes overall customer classification process. The parallelized algorithms have resulted in appreciable results as displayed in the results section.

Smart meters have not only allowed for efficient management of many end-users, but also have made AMI an attractive target for remote exploits and local physical tampering with the end goal of stealing energy. While smart meters posses multiple sensors and data sources that can indicate energy theft, in practice, the individual methods exhibit many false positives. In this paper, we present AMIDS, an AMI intrusion detection system that uses information fusion to combine the sensors and consumption data from a smart meter to more accurately detect energy theft. AMIDS combines meter audit logs of physical and cyber events with consumption data to more accurately model and detect theft-related behavior. Our experimental results on normal and anomalous load profiles show that AMIDS can identify energy theft efforts with high accuracy. Furthermore, AMIDS correctly identified legitimate load profile changes that more elementary analyses classified as malicious.

There are two types of losses i.e. technical and nontechnical during the process of generation, transmission and distribution of electrical energy. There is dissipation of energy in transmission lines and other power components. One of the main reasons of non-technical losses comes from electricity theft. It generally involves bypassing the distribution feeder, tampering with energy meter or using other physical methods, Power utilities lose large amount of money each year because of fraudulent electric customer. Electricity theft can be defined as a deceitful or illegal usage of electric equipment or services with the purpose to avoid billing charges. It is not possible to stop theft completely, however measures can be taken to identify, prevent and reduce fraud. Recently, detecting the fraudulent electricity customer has been an active area of research. This is a problem faced by almost all power utility companies. This paper presents a novel idea of detection of power theft using probabilistic neural networks (PNN). This model selects the suspected customer on the basis of its electricity consumption behaviour. The probabilistic neural network algorithm represents the likelihood function of given class as the sum of same isotropic Gaussians. Twelve monthly power consumption details are given as input to neural network, which is trained to give the desired output.

The distribution losses in power utilities originating from electricity theft and other customer malfeasances are called nontechnical (NTLs). These losses mainly occur due to meter tampering, meter malfunction, illegal connections, billing irregularities, and unpaid bills. This letter extends previous research work in modeling a nontechnical loss (NTL) framework for the detection of fraud and electricity theft in power distribution utilities. Previous work was carried out by using a support vector machine (SVM)-based NTL detection framework resulting in a detection hitrate of 60%. This letter presents the inclusion of human knowledge and expertise into the SVM-based fraud detection model (FDM) with the introduction of a fuzzy inference system (FIS), in the form of fuzzy IF-THEN rules. The FIS acts as a post processing scheme for short-listing customer suspects with higher probabilities of fraud activities. With the implementation of this improved SVM-FIS computational intelligence FDM, Tenaga Nasional Berhad Distribution’s detection hitrate has increased from 60% to 72%, thus proving to be cost effective.

III. PROPOSED SYSTEM

Electricity is produced and transmitted using power grids. The power grids are the distributed networks established near energy resources. The grids consume that energy to produce electricity. The power grid network consists of smart grids that help to transmit that produced electricity to the consumers. These smart grids have smart sensors or meters which take and store information about the electricity consumption usage and statistics. Smart grids bring the combined features of big data and edge computing. As it allows to analyzing large amount of data that is collected by smart sensors, hence, these smart meters are vulnerable to malicious attacks. These attacks usually occur by hacking the electric meter, misconfiguration of the meter or bypassing the electric meter and forcing it to produce fake readings. These fake readings further affect the efficiency, quality and transmission of the electricity. Therefore, the security of smart grids is very important. Hence, the CNN2D model is proposed in this paper to overcome these problems.

The dataset used for this purpose is released by State Grid Cooperation of China (SSGC) which is one of the largest cooperation of China with all the electricity consumption data records. The dataset consists of the electricity consumption data of 42372 customers within two years (i.e., 2014-2016). The data observe from the daily consumption that the daily data has many fluctuations which make it difficult to detect the fraudulent behavior. Therefore, I convert one-dimensional daily consumption data to two-dimensional weekly consumption data.

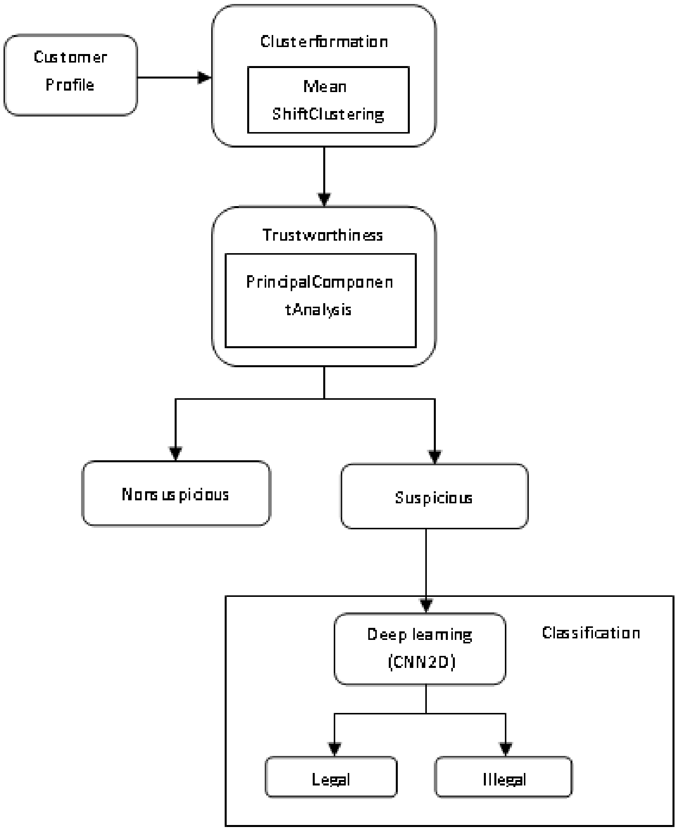


Fig.3.1 System Architecture

This work presents a computational method that uses energy consumption measurement patterns to detect illegal residential consumers in a smart grid environment. In general, electronic meters (smart meters) collect real-time information from the consumers several times per day. Despite the numerous daily residential load profiles that appear, due to the examination over a long time period an artificial dataset with near real-time energy consumption patterns has been developed in this work. Furthermore, the well-known clustering algorithm mean shift along with a number of applications in the power theft detection field, has been proposed and implemented, which in Legal Deep learning (CNN) Illegal Classification Customer profile Cluster formation Mean Shift Clustering Trustworthiness Principal Component Analysis Non suspicious Suspicious combination with PCA analysis successfully maps residential energy consumption patterns in terms of legal and illegal. The NTL methods based on artificial intelligence are typically applied to features computed from customer electricity consumption profiles and require the feature extraction from historical data for training process. The computational effort for the feature extraction from historical data is not necessary when combining PCA data analysis with mean shift clustering algorithm. Define from the available Smart meter data, the customer profile data of a specific area is chosen. It is believed that all the customers of the selected region are genuine profiled. Given that the mean shift is an unsupervised clustering algorithm it can perform clustering to any amount of historical data available. After finding the trustworthiness of the customers, the genuine profiled customers are considered for the classification model by including the bogus data into actual data. The deep CNN block consists of 2-D input which is connected to many convolution layers and pooling layers. The 1-D input of wide component is converted to 2-D in terms of weeks. This 2-D input is then passed through the convolution 2-D model. The outputs of both the wide CNN and deep CNN are then passed to the fully connected layer. Fully connected layer has an activation function which activates the required neurons. Both the outputs are merged and passed in the form of inputs with some weights. As all the neurons are connected to each other so it takes the input values and their weights to train the model.

TRUSTWORTHINESS OF CUSTOMERS

Define from the available Smart meter data, the customer profile data of a specific area is chosen. It is believed that all the customers of the selected region are genuine profiled. The percentage of trustworthiness of the customers is identified by using machine learning algorithm. For this purpose, unsupervised k-means clustering algorithm is applied. The clustering is performed to select the customer’s profile which is more genuine in their power usage pattern by grouping them in clusters. The customers are clustered based on their power usage readings obtained from their smart meter. For this purpose, a sample customer’s smart meter reading for every 30 minutes in (KWH) for 28 days is considered. The customers profile dataset is given as input to k-means clustering algorithm. The k-means clustering algorithm will cluster these customers into k clusters. The customer’s profile that is close enough to the cluster head is the final selected customers for the theft detection task. These customers are identified as trustworthy customers.

MEAN SHIFT CLUSTERING

Initially the customers profile is clustered based on the feature values (smart meter reading). The Mean-Shift clustering algorithm specify the number of expected cluster. Mean shift algorithm is a nonparametric clustering technique which does not require prior knowledge of the number of clusters, and does not constrain the shape of the clusters. Mean shift algorithm considers data points as a sample of a probability density function. If dense regions (or clusters) are present in the feature space, then correspond to the mode (or local maxima) of the probability density function. For each data point, mean shift algorithm associates it with the nearby peak of the dataset’s probability density function. For each data point, mean shift algorithm defines a window around it and computes the mean of the data point. Then it shifts the center of the window to the mean and repeats the algorithm till it converges. After each iteration, the window shifts to a denser region of the dataset.

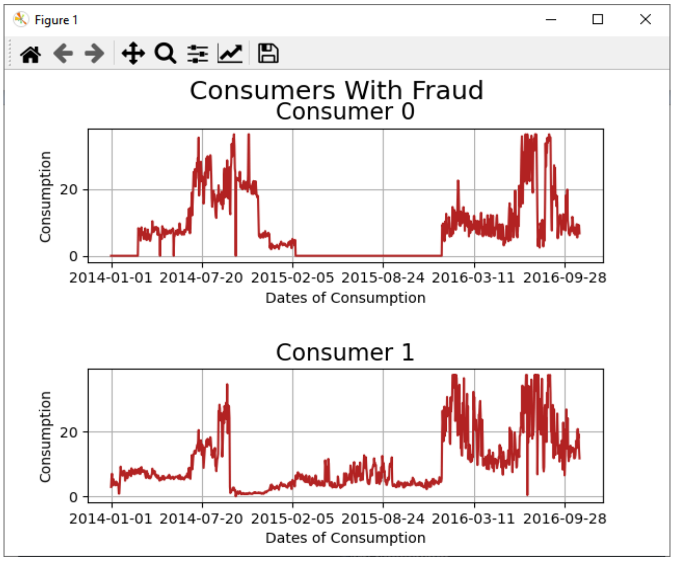
SMART METER DATA ANALYTICS

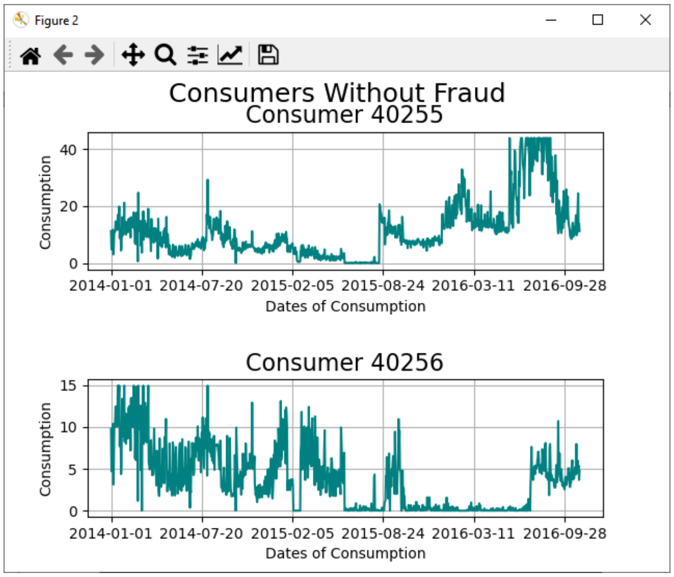
The genuine customers profile is obtained from the result of Mean-shift clustering. For each customer, the smart meter reading is obtained for every half an hour. This sampling rate is reduced to one reading (average reading of 48 readings of a day) per day per customer. For each of the considered sample in dataset, three types of bogus data samples are generated for every day reading. In type 1, a random value is generated between -0.5 and 0.5. This random value is multiplied with the average reading value calculated for per day. It replicates the acceptable change in meter reading. This is done for all 28 days readings of all sample customers considered for the experiment. In type 2, random days are taken where the actual data values are replaced with zero. This implies the scenario where the meter does not work. In type 3, the mean value of 28 days readings are multiplied with the each of the day reading.

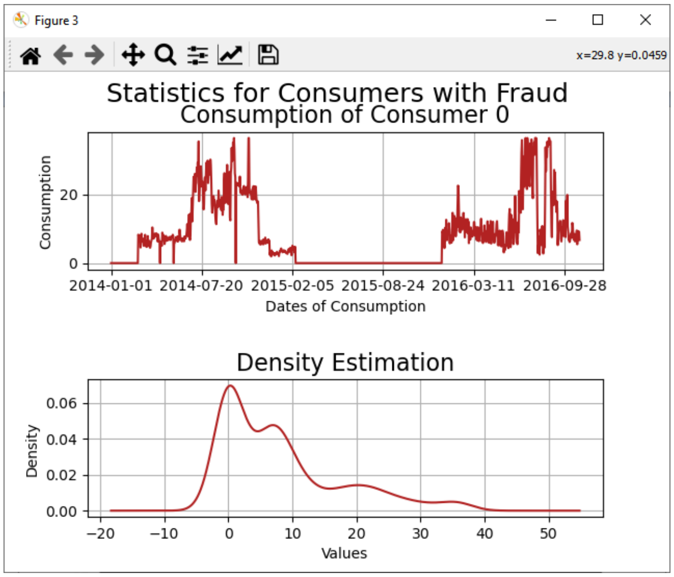
CLASSIFICATION

After finding the trustworthiness of the customers, the genuine profiled customers are considered for the classification model by including the bogus data into actual data. The Convolution Neural Network is built to classify the customer's profile. The three types of bogus data along with the actual data are considered to train the neural network. 60% of the dataset is utilized for training the neural network. After required number of iterations, the neural network is trained to predict any new customer profile to genuine or fraud. The remaining 40% of the dataset is used for testing the dataset. The prediction is made by the CNN2D classification model. The performance of the proposed system is using two parameters namely accuracy and error rate. The difference in actual class value and the predicted class value is considered for the performance evaluation. The performance of the model depends on the number of dataset taken into consideration.

IV. RESULT AND DISCUSSION







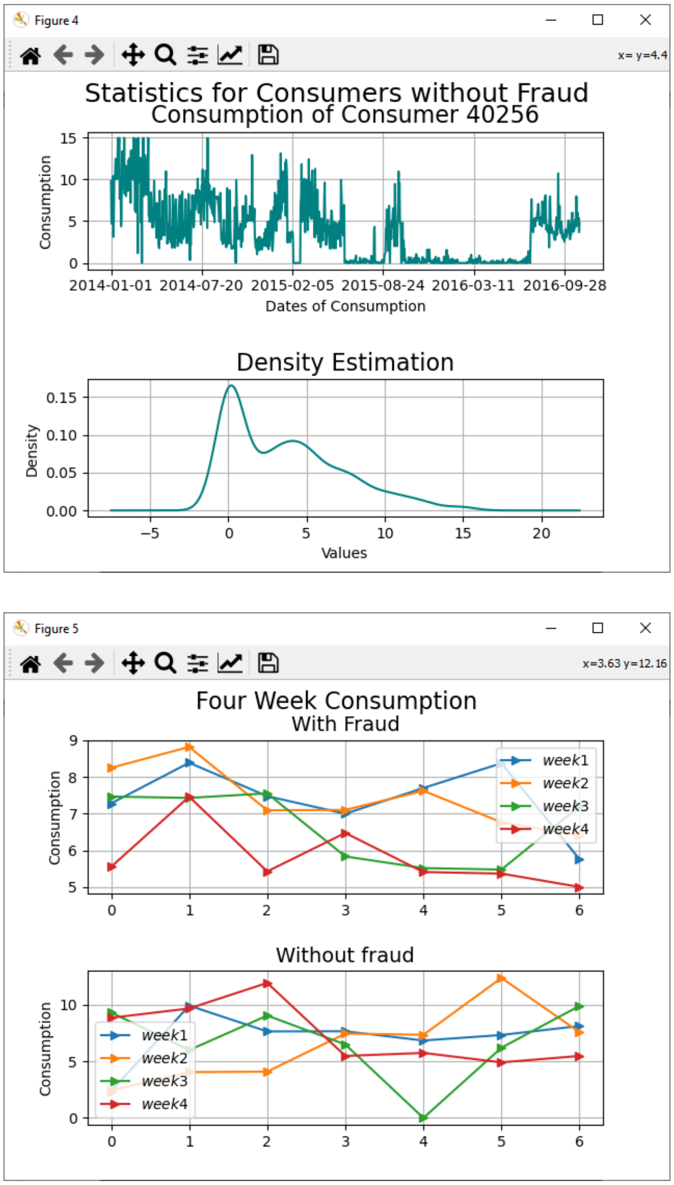
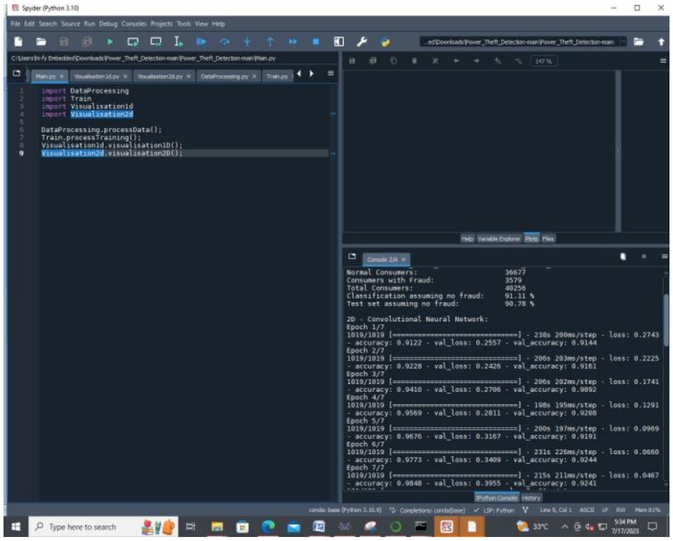


Figure 4.1 Preprocessing Data



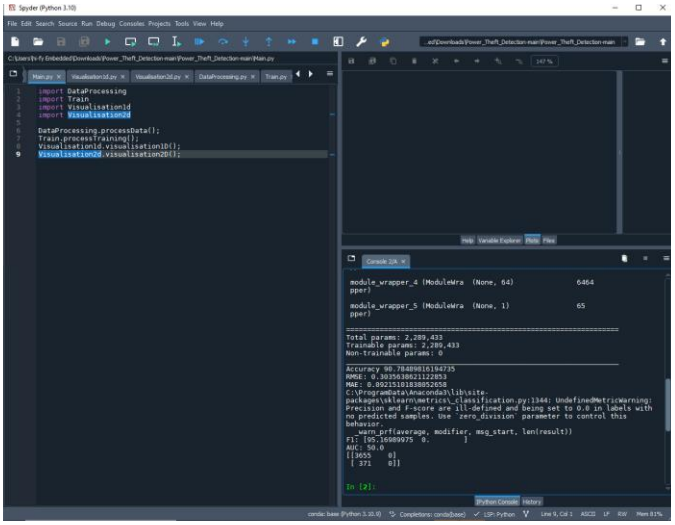
```
import DataProcessing
import Train
import Visualisation1d
import Visualisation2d

DataProcessing.processData();
Train.processTraining();
Visualisation1d.visualisation1D();
Visualisation2d.visualisation2D();
```

```
Normal Consumers:                     36677
Consumers with Fraud:                 3579
Total Consumers:                      40256
Classification assuming no fraud:     91.11 %
Test set assuming no fraud:           90.78 %

2D - Convolutional Neural Network:
Epoch 1/7
1019/1019 [==============================] - 238s 200ms/step - loss: 0.2743
- accuracy: 0.9122 - val_loss: 0.2557 - val_accuracy: 0.9144
Epoch 2/7
1019/1019 [==============================] - 206s 203ms/step - loss: 0.2225
- accuracy: 0.9228 - val_loss: 0.2426 - val_accuracy: 0.9161
Epoch 3/7
1019/1019 [==============================] - 206s 202ms/step - loss: 0.1741
- accuracy: 0.9410 - val_loss: 0.2706 - val_accuracy: 0.9092
Epoch 4/7
1019/1019 [==============================] - 198s 195ms/step - loss: 0.1291
- accuracy: 0.9569 - val_loss: 0.2811 - val_accuracy: 0.9208
Epoch 5/7
1019/1019 [==============================] - 200s 197ms/step - loss: 0.0969
- accuracy: 0.9676 - val_loss: 0.3167 - val_accuracy: 0.9191
Epoch 6/7
1019/1019 [==============================] - 231s 226ms/step - loss: 0.0660
- accuracy: 0.9773 - val_loss: 0.3409 - val_accuracy: 0.9244
Epoch 7/7
1019/1019 [==============================] - 215s 211ms/step - loss: 0.0467
- accuracy: 0.9848 - val_loss: 0.3955 - val_accuracy: 0.9241
```

Figure 4.2 Training Model



```
import DataProcessing
import Train
import Visualisation1d
import Visualisation2d

DataProcessing.processData();
Train.processTraining();
Visualisation1d.visualisation1D();
Visualisation2d.visualisation2D();
```

```
 module_wrapper_4 (ModuleWra  (None, 64)               6464
 pper)

 module_wrapper_5 (ModuleWra  (None, 1)                65
 pper)

=================================================================
Total params: 2,289,433
Trainable params: 2,289,433
Non-trainable params: 0
_________________________________________________________________
Accuracy 90.78489816194735
RMSE: 0.3035638621122853
MAE: 0.09215181838852658
C:\ProgramData\Anaconda3\lib\site-
packages\sklearn\metrics\_classification.py:1344: UndefinedMetricWarning:
Precision and F-score are ill-defined and being set to 0.0 in labels with
no predicted samples. Use `zero_division` parameter to control this
behavior.
  _warn_prf(average, modifier, msg_start, len(result))
F1: [95.16989975  0.        ]
AUC: 50.0
[[3655    0]
 [ 371    0]]

In [2]:
```

Figure 4.3 Classification result

Table 4.1 Classification

Method	Accuracy	Precision	Recall	F-score	AUC
CNN	0.88	0.86	0.48	0.14	0.5
CNN2D	0.92	0.92	0.54	0.15	0.54

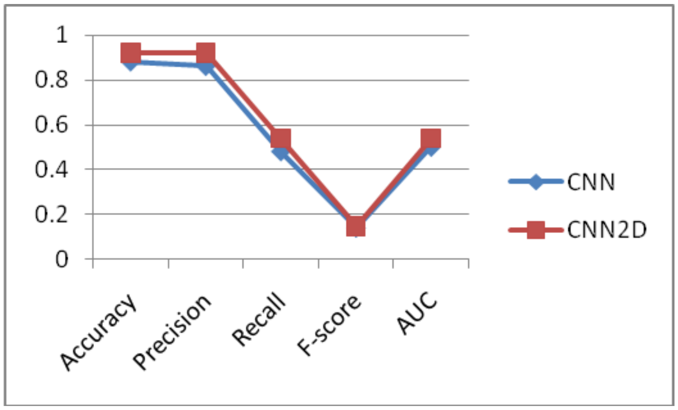


Figure 4.4Classification

V. CONCLUSION

This project proposes CNN2D model to identify electricity theft in smart grids. In particular, I designed a deep learning model for electricity theft detection which is based on convolutional neural network. The main advantage of using CNN2D is that these neural networks extract all the important features of the data without any human supervision. The CNN2D model consists of input layers, hidden layers and the output layer. The output layer of the CNN model to enhance its results in terms of accuracy. The experimental results have shown that our proposed model achieved 92% accuracy, which is better than state-of-art models.

The model is trained on a limited number of datasets without incorporating additional non-sequential parameters, which limits its ability to detect theft. In addition, low-sampled data is included, which impacts the performance of the proposed model while obtaining finer-grained information on energy theft. For the reliable detection of energy thieves in the future, we will thus consider high-sampling data and other non-sequential data. Moreover, other evaluation indicators for electricity theft detection, such as MAP@100 and MAP@200 will be used in future studies.

REFERENCES

[1] S. Foster, Non-Technical Losses: A \$96 Billion Global Opportunity for Electrical Utilities, Nov. 2021, [online] Available: https://energycentral.com/c/pip/non-technical-losses-96-billion-global-opportunity-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", Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), pp. 2138-2142, Jun. 2020.

[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, E-Meters Offer Multiple Ways to Combat Electricity Theft and Tampering, Nov. 2021, [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", Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), pp. 1-6, Apr. 2018.

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

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

[10] 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, Global Smart Grid Market Size by Region 2017–2023, Mar. 2022, [online] Available: https://www.statista.com/statistics/246154/global-smart-grid-market-size-by-region/.

[12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai and Y. Zhou, Electricity Theft Detection, Sep. 2021, [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.

[15] S. B. Yousaf, M. Jamil, M. Z. U. Rehman, A. Hassan and S. O. G. Syed, "Prototype development to detect electric theft using PIC18F452 microcontroller", Indian J. Sci. Technol., vol. 9, no. 46, pp. 1-5, Dec. 2016.

[16] Dineshkumar, P. Ramanathan and S. Ramasamy, "Development of ARM processor based electricity theft control system using GSM network", Proc. Int. Conf. Circuits Power Comput. Technol. (ICCPCT), pp. 1-6, Mar. 2015.

[17] S. Ngamchuen and C. Pirak, "Smart anti-tampering algorithm design for single phase smart meter applied to AMI systems", Proc. 10th Int. Conf. Electr. Eng./Electron. Comput. Telecommun. Inf. Technol., pp. 1-6, May 2013.

[18] Khoo and Y. Cheng, "Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis", Proc. Wireless Telecommun. Symp. (WTS), pp. 1-6, Apr. 2011.

[19] Astronomo, M. D. Dayrit, C. Edjic and E. R. T. Regidor, "Development of electricity theft detector with GSM module and alarm system", Proc. IEEE 12th Int. Conf. Humanoid Nanotechnol. Inf. Technol. Commun. Control Environ. Manage. (HNICEM), pp. 1-5, Dec. 2020.

[20] P. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns", IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 216-226, Jan. 2015.