e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

AN EFFICIENT EXTRA-TREE CLASSIFIER BASED APPROACH FOR DETECTING NON-TECHNICAL LOSSES IN POWER UTILITIES

Mujeeb Ali*1, Dr. Touqeer Ahmed Jumani*2, Dr. Zohaib Leghari*3, Engr. Safdar Abro*4

*1,2Electrical Power Engineering Department, Mehran Unversity Of Engineering And Technology, SZAB Campus Khairpur, Sindh, Pakistan.

*3Electrical Engineering Department Mehran University Of Engineering And Technology Jamshoro, Pakistan.

*4Electrical Department Benazir Bhutto Shaheed University Of Technology And Skill Development Khairpur, Pakistan.

DOI : https://www.doi.org/10.56726/IRJMETS45482

ABSTRACT

Non-technical losses (NTLs) have been proved to be one of the most challenging concern for electricity distribution companies. Billions of dollars have been projected each year as a result of these criminal actions. There are plenty of causes behind these non-technical losses. One of the biggest reasons is still the use of Traditional time-consuming and inefficient NTL detection methods by power distribution companies around the world, particularly in developing countries. This study aims to address the above-mentioned issue by building an effective energy theft detection model for detecting fraudulent users in a power distribution system. The primary goal of this research is to support distribution system operators in their fight against energy theft.

To begin, the proposed computational model Extra-tree classifier Technique is used and number of diverse features which were extracted from monthly consumer consumption data that is obtained from MEPCO to distinguish between honest and fraudulent customers. For many years, electricity theft and energy consumption fraud have been major issues for power distribution companies (PDC). PDCs all over the world are experimenting with various methods for detecting electricity theft. Traditional methods for detecting NTLs, such like on-site inspection and reward and penalty policies, have fallen out of favor in the modern era due to their ineffective and time-consuming methods.

Keywords: Non-Technical Losses (Ntls), Power Distribution Companies (PDC), Electricity Theft.

I. INTRODUCTION

There are operational losses in each of the three primary components of the power system: generation, transmission, and distribution. The losses on the transmission and distribution (T&D) side of the power system are incalculable, in contrast to the losses on the generation side, which can be calculated with precision. This is because there are numerous non-technical energy losses associated with T&D in addition to technical energy losses. Technical losses are the result of power dissipation in various power system components, including transmission lines, transformers, electrical appliances, switches, and many other power system components. . Only two parameters, total grid load and total energy bill, need to be measured in order to calculate these losses. Losses On the other hand, NTL covers mistakes in billing, subpar infrastructure, broken equipment, supplies without meters, and illegal consumer behavior like theft, corruption, and organized crime. NTLs are more difficult to predict than technical losses, making their reduction one of the top priorities for any PDC. In the worst-case scenarios, nearly half of the total electrical power generated is converted into NTLs, resulting in billions of dollars in annual losses. A $25 billion annual cost is attributed to electricity theft by utility companies worldwide. The above-said issue existed in almost all countries. However, its consequences are more severe in developing countries than in developed [1]. For example, for utilities in Pakistan, T&D losses were recorded at 17.5 percent for the fiscal year 2017–2018, [2] causing significant damage to the country's feeble economy and are significantly higher than in other Asian countries such as China and Korea, where T&D losses were recorded at 8 percent and 3.6 percent, respectively. NTL losses are estimated to account for 33% of total T&D losses in the country's electrical system [2]. In general, PDCs used to inspect metering equipment based on observations discovered through a chance analysis of consumer billing profiles to find NTLs. Since consumer behavior and consumption patterns are not taken into account during the detection process, such random inspections have a very low success rate. The mentioned process is also ineffective and inefficient for detecting theft because only a random sample of the bills are chosen for inspection, leaving many others unnoticed. This is due to the random nature of the process. This approach's price tag and time commitment are two other serious drawbacks. [3]. This is because the distribution feeders in developing countries typically have very long lengths and supply a sizable number of consumers. Recently, one of the most practical options for reliable NTL detection has been smart meters with dedicated communication links. They are an impractical option for many developing nations, including Pakistan, due to their enormous installation and maintenance costs. NTL detection in Pakistani PDCs has not received much attention despite being one of the most significant threats to the nation's economy, which is the main driver behind the present study. In this work, the Extra-tree classifier ensemble learning technique for energy theft detection is proposed. To the best of my knowledge, a novel feature extraction and feature selection-based process for delivering insightful information about customers' energy usage behavior is a novel technique that has only recently been used a very small amount.[4] However, given that they require billions of dollars in installation and maintenance, many developing nations, including Pakistan, cannot afford them. The lack of research on NTL detection in Pakistani PDCs despite being one of the most significant threats to the nation's economy is the main driver behind the present study. This study suggests using an ensemble learning technique called Extra-tree classifier to identify energy theft. As far as I'm aware, a novel feature extraction and feature selection-based process for delivering insightful data about customers' energy usage behavior is a novel technique that hasn't been used much thus far[5]. The method just described helps to distinguish between healthy and fraudulent customers in an efficient manner, increasing the likelihood of detection and reducing the need for an expensive and time-consuming inspection. Utilizing data on energy consumption provided by the State Grid Corporation of China, the proposed Extra-tree classifier approach distinguishes between dishonest and honest customers (SGCC). Although, as was previously stated, there are numerous contributing factors to NTLs, this research considers feature-based analysis, which yields superior and realistic results, as supported by the study's findings, in contrast to earlier research that saw the sudden deviation in energy consumption as the only indication of fraud. . At the conclusion of the suggested method, the shortlisted fraudster customers must be examined in person in order to catch the wrongdoers. Following that, a physical inspection will be conducted using the records of potentially fraudulent customers. By avoiding frequent on-site physical inspections, the proposed method is anticipated to reduce operational costs for power companies while also significantly increasing NTL detection rate

NTLs plaguing Power Distribution companies

Worries over non-specialized misfortunes (NTLs) have tormented influence dissemination organizations (PDCs). False charging, metering, and purchaser conduct cost the economy billions of dollars consistently. To distinguish NTLs and diminishing NTL, PDCs much of the time review buyer charging profiles and assess metering hardware at arbitrary. Nonetheless, this absence of information on purchaser conduct or utilization designs, which brings about an extremely low discovery rate, is the fundamental weakness of these inconsistent reviews and examinations. Moreover, these customary review and examination methods are ineffectual on the grounds that circulation feeders in emerging countries are regularly extremely lengthy and have countless buyers, making them often extravagant and tedious. From that point forward, one of the most up to date advancements is brilliant meters.

- Normal calculations like (SVM, KNN, Strategic Relapse, GB, and Choice trees) are frequently one-sided and have restrictions in exactness, accuracy, and review for non-specialized misfortune discovery. To beat these issues, a more viable calculation is utilized, decreasing inclination and further developing exactness, subsequently offering a promising answer for exact power burglary identification.
- Information adjusting procedures like (arbitrary oversampling, irregular under sampling) frequently bring about one-sided forecasts and incorrect exactness evaluations. To amend this, it's fundamental to embrace information adjusting strategies that limit expected predispositions and yield steadier, less one-sided expectations.

• Approval approach should be consolidated, guaranteeing the model's compelling recognition of non-specialized losses (Power burglary) while maintaining information quality and dependability.

Nagi et al. (2009) [6] used factors like monthly spending data and creditworthiness rating to train the SVM model to distinguish between dishonest and legitimate consumers. In the earlier work, a Fuzzy Inference System (FIS) was utilized with SVM to boost the detection rate. Nizar et al (2008) [7] made use of the Online Sequential Extreme Learning Machine (OS-ELM) for locating NTL activities. Costa et al. (2013) [8] presented artificial neural networks (ANN) for non-technical losses identification. In order to categorize the consumers as honest or dishonest, the authors created a database using the customer's energy use data. Glauner et al. (2016) [9] used fuzzy logic, SVM, and Boolean rules to recognize the NTL behavior. Data on energy use over a 12-month period was utilized by the authors to train the algorithm. They added characteristics such geographic position and inspection notes to the suggested classifier in order to compute the NTL in the neighborhood, further enhancing its performance. Guerrero et al (2018) [10] boosted the detection rate by using two coordinate modules. For customer filtering in the first module, text mining and ANN were employed, and in the second module, classification and regression (C&R) trees and self-organizing map (SOM) neural networks were used. Leite et al (2016) [11] developed a multivariate control chart to determine the NTL brought on by various kinds of cyber-attack. Additionally, the location of the fraudulent customer was later determined using the A-Star algorithm.

Buzau et al. (2018) [12] proposed the algorithm of Boost, which detects NTL using auxiliary databases in addition to the smart meter dataset.

Tariq et al (2016) [13] proposed a Stochastic Petri net formalism to locate NTL in grid-tied micro-grids. The arc is set off by a change in the resistance value above a specific threshold, and the Meter Data Management System (MDMS) uses information from the tempered meter to identify the fraud as a result. A Gradient Boosting Theft Detector (GBTD) approach was proposed by the authors in reference, and it is based on three different boosting classifiers which are Light Gradient Boosting (LGBoost), Categorical Boosting (CatBoost), and Extreme Gradient Boosting (XGBoost).

Weckx et al (2012) [14] presented a linear model using voltage and power measurements in order to detect NTL. Zheng et al (2018) [15] worked on a wide and deep convolutional neural network model to observe the NTL in smart grids. The proposed method was demonstrated to perform better than other popular techniques including SVM, LR, RF, and ANN. To address the NTL problem, the authors suggested a brand-new correlation analysis-based approach. The key benefit of the suggested plan is that the model may be trained without using tagged data. Halabi et al (2019) [16] created a low-cost NTL detection technique that can spot energy thieves instantly and without a delay. The suggested plan protects energy consumers' privacy by deleting the high-vccresolution data on instantaneous power. Kim et al (2021) [17] proposed a model for identifying NTL using an intermediate monitor meter and analysis of power flow. Gao et al (2019) [18] worked on a data-driven model with a physical influence that was based on data from smart meters on voltage and energy usage. By creating a linear link between voltage magnitude and power usage, the suggested method detects NTL behavior. To prevent pointless inspections, the authors suggested a suspicion assessment-based inspection algorithm. By examining the discrepancy between predicted and reported consumption, the energy behavior of the consumers is thoroughly examined. Messinis et al (2019) [19] built a model which accurately detects NTL in the distribution grid using power system optimization, voltage sensitivity and SVM. Massaferro et al (2020) [20] proposed RF to detect NTL. The proposed scheme's experimental findings demonstrated that algorithms of machine learning can significantly boost economic returns. In another study, Nabil et al (2019) [21] suggested an energy theft detection system for the Advanced Metering Infrastructure (AMI) network that protects privacy. To enable the energy customers to submit the disguised reading to system operators for monitoring and invoicing purposes, the scheme uses a secret sharing approach.

1. To develop a feature engineered Extra-tree classifier-based theft detection framework for identifying the fraudster consumers in a labeled dataset
2. To improve the generalization capability of the developed theft detection framework using SMOTE-ENN.

Machine learning is an AI application. It is the process of employing mathematical data models to assist a

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

computer in learning without direct instruction. This allows a computer system to learn and improve on its own, based on past experience. Many applications and businesses employ machine learning in their day-to-day operations because it is more accurate and exact than manual interventions. Following are diagram show the step wise procedure.

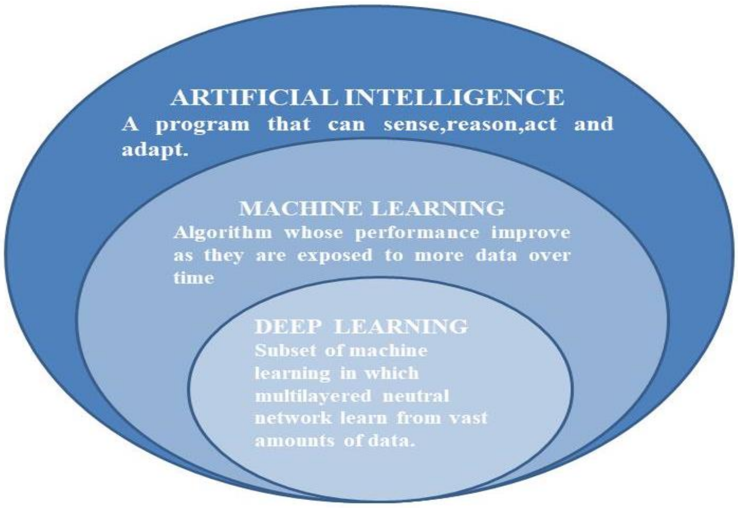

Fig 1: Model Of AI

II. METHODOLOGY

SAMPLING METHODOLOGY

The complete methodology of presented study is mentioned and explained in below shown flowchart, the overall framework in divided into three main stages.

1. Data pre-processing stage
2. Feature engineering
3. Model training and evaluation stage.

1. Data pre-processing stage:

In Data pre-processing stage we convert the raw data into a meaningful and understandable data structure. The proposed theft detection model is tested using the electricity consumption data which is acquired from MEPCO dataset, following the acquisition of data, the daily electricity consumption of 2762 consumers was calculated for a period of approximately 1127 days. It is comprised of 76.65 percent honest customers and 23.35 percent theft customers.

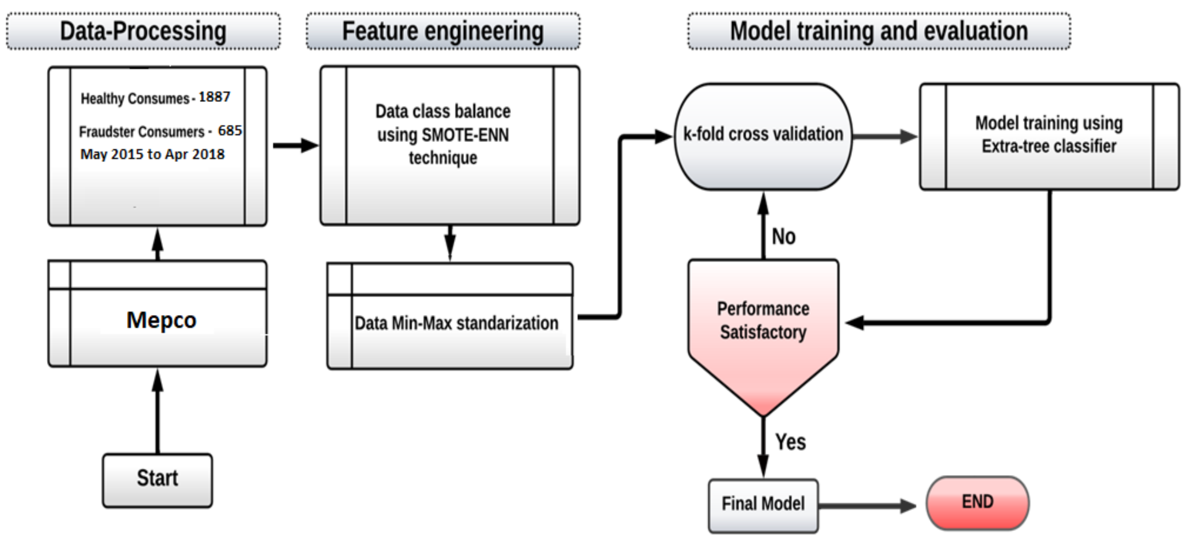

Fig 2: Flowchart of the proposed study

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Data class balancing and feature engineering:

This second stage is divided into two sub-stages:

- Data class balancing
- Feature engineering

Data class balancing: The Data set which we getting for the current study is in unbalanced form therefore it is essential to balance the class distribution before the feature extraction and selection process, so in order to solve this issue we have used the SMOTE-ENN technique. SMOTE-ENN technique will attenuate the imbalanced data class distribution issue. Within the realm of addressing class imbalances in datasets, the SMOTE-ENN approach presents a valuable solution. This technique combines the strengths of two distinct methods to combat the common challenge of uneven class distribution. SMOTE, which stands for Synthetic Minority Over-sampling Technique, is utilized to bolster the minority class by generating synthetic data points, effectively mitigating the issue of imbalance. Nonetheless, the synthetic instances introduced by SMOTE can at times introduce noise into the dataset, potentially hampering model performance. It is at this juncture that ENN, or Edited Nearest Neighbors, comes into play. ENN acts as a post-processing filter, diligently sifting through the data to enhance its quality. It achieves this by pinpointing and removing instances that are either noisy or erroneously classified within the minority class.The combined approach of SMOTE for over-sampling or ENN for data purification synergizes to create a dataset that not only achieves balance between classes but also fine-tunes the data quality. By eliminating instances that have the potential to introduce noise or misclassification, the SMOTE-ENN strategy results in an improved dataset. This optimized dataset, in turn, facilitates the development of machine learning models that are both more robust and accurate when confronted with imbalanced datasets Feature engineering is that the process of extraction and selection of the foremost important features from given data, that dataset are extracted using feature extraction and selection process

Model training and evaluation stage: This third stage is further divided into three sub-stages

- Performance evaluation metrics
- Extra tree classifier algorithm
- Proposed model's outcomes interpretability using the Extra tree classifier Technique. According to below block diagram we Test the multiple Factor like a temperature, Monthly consumption in tree classifier got accuracy 82%.

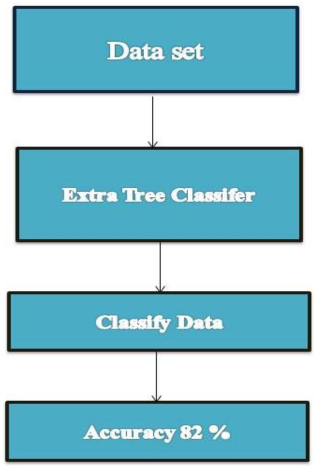

Fig 3. Flowchart of Extra tree classifier

ERT requires careful tuning of hyper parameters like tree number, depth, and sample count for optimal performance, using Cross-validation and grid search techniques. Talk about the ERT model's implementation details for detecting electricity.

Theft, in the cited research, a supervised method is used to train an Electricity Theft Detection (ETD) classifier model. A Labeled Smart Meter (SM) dataset was used to train the model. This dataset contains daily electricity consumption Information from both theft and legitimate users. The data preprocessing, model training, and model evaluation stages can be used to broadly categorize the entire framework for detecting electricity theft Here is a description of each phase.

Preprocessing Data:

- Data preprocessing entails getting the SM dataset ready for the ETD classifier model's training.
- Steps in this phase include feature engineering, normalization, and data cleaning.
- The process of handling missing values, outliers, and resolving any discrepancies in the dataset is known as data cleaning
- In order to prevent some features from overpowering the model training process, normalization makes sure that the data is scaled appropriately.
- To improve the functionality of the model, feature engineering may entail extracting pertinent features, transforming the data, or including additional contextual information.

Experimental Setup and Evaluation:

- The ETD classifier model is evaluated after training to determine how well it performs in identifying electricity theft.
- In the evaluation stage, the generalization ability of the model is tested using a different dataset, such as a holdout set or cross-validation.
- The efficacy of the model is assessed using performance metrics like accuracy, precision, recall, F1 score, or ROC curve analysis.
- The evaluation's findings shed light on the model's capacity to accurately detect theft while minimizing false alarms.

Detecting electricity theft requires data from distribution systems like smart meters and utility companies, with methods varying based on resources and data-sharing agreements.

1 Smart Meters:

- Electricity consumption is monitored regularly by smart meters, which are electronic devices installed at customer locations.
- Smart meters can automatically collect data because they are made to transmit consumption information to utility companies or data aggregators.
- Utility companies can provide access to anonym zed or aggregated smart meter data for research purposes.

2 Utility Companies:

- For billing and other operational reasons, utility companies gather and keep a lot of records about electricity consumption.
- Collaborating with utility companies allows researchers to analyze large-scale energy usage patterns, gain valuable insights, and ensure privacy protection for individual consumers, benefiting both parties.

3 Research Datasets:

- Datasets relating to electricity consumption are made publicly available by some research institutions or governmental organizations.
- These datasets could contain information on past consumption patterns, weather patterns, or demographics

4 Data Preprocessing and Integration:

- Once the data has been collected, preprocessing procedures might be necessary to clean and convert the raw data into a usable format.
- Data cleaning includes handling outliers, handling missing values, and resolving discrepancies in the data.
- To add more features or contextual information to the dataset, it might be necessary to integrate data from various sources.

It's important to remember that the precise data sources and collection techniques can change depending on the jurisdiction, data accessibility, and data-sharing policies. When gaining access to and utilizing data on electricity consumption, researchers should make sure that all ethical standards, privacy laws, and any

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

required approvals or permissions are followed.

III. RESULTS AND DISCUSSION

We have obtained monthly electric power consumption data of more than 2762 from a distribution company. Graph no.1 below gives the month wise power consumption of consumers. This data also gives the status as "Healthy" which means there is no theft found and "Theft" which means there is any discrepancy or suspected theft is found at the user end. Apart from consumption, the data also contains the average temperature of that month. We can relate the consumption from the temperature and found that when the temperature is high the consumption is also increased.

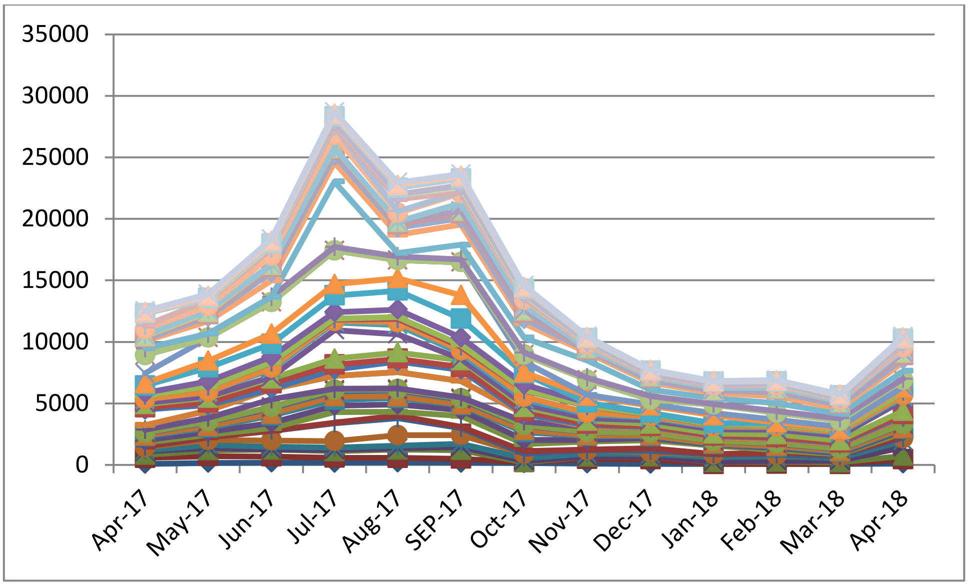

Fig 4: Graph Show Consumer Wise Monthly Consumption

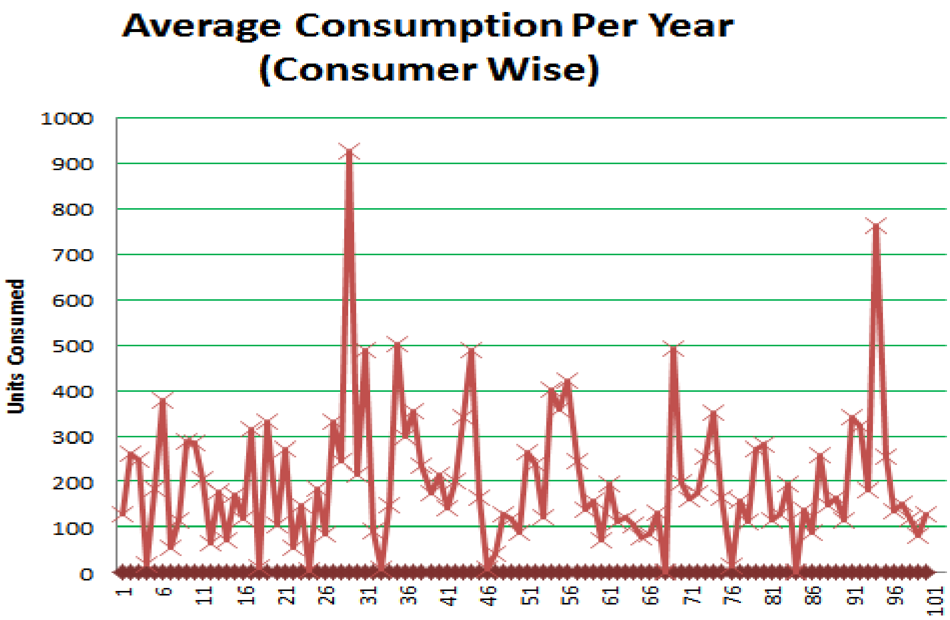

Fig 5: Graph shows the per year average usage of consumers.

Figure 6 shows the month wise average consumption by the consumers in graphs. Shows in figure.7 Graph shows the percentage of consumption throughout the year.

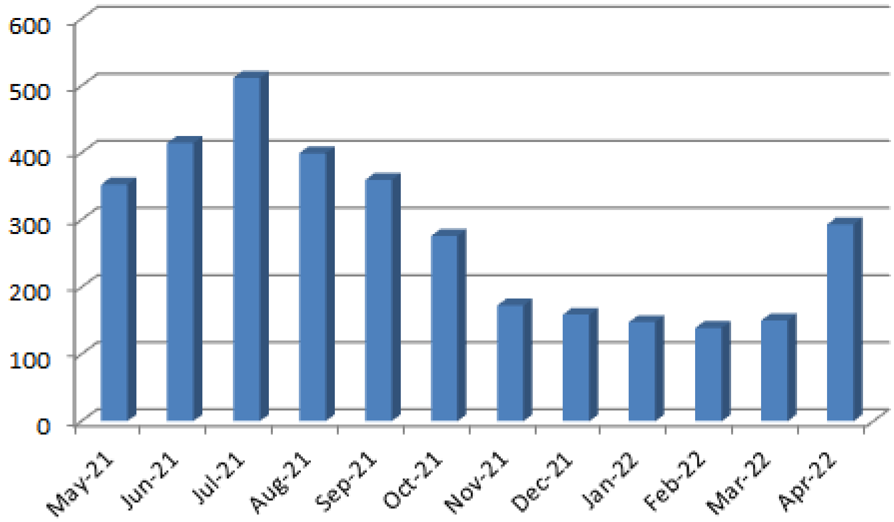

Fig 6: Graph shows Month wise average consumption per consumer

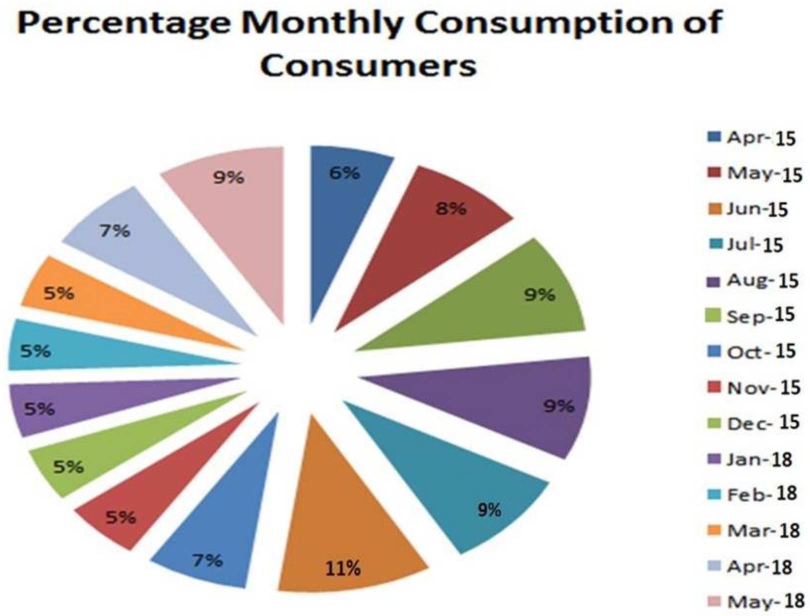

Fig 7: Graph shows Percentage monthly Consumption

This given data set is used to train the machine learning model by using Extra tree classifier. The accuracy of the classifier is 82% while precision of the classifier is 82% and 82% for true positive and true negative outputs respectively. The recall for true positive outputs was found to be 74% and for true negatives outputs it is 88%. F1 score for decision tree classifier is 78% and 85% for true positive and true negative outputs respectively.

After collected monthly electric power consumption data from 2,762 consumers via MEPCO. Applying an Extra-Tree Classifier to this dataset, we were able to classify consumers into two distinct categories: "Healthy" and "Theft." In our analysis, 76.65% of consumers were categorized as "Healthy," indicating that no signs of theft were detected in their power consumption patterns. These consumers displayed consistent and expected electricity usage. On the other hand, 23.35% of consumers were classified under the "Theft" category. This designation implies that their power consumption patterns raised concerns of potential theft or suspicious activities at their end. Further investigation or monitoring may be necessary for this subset of consumers. This classification using the Extra-Tree Classifier offers valuable insights for identifying potential issues with electricity consumption, allowing for a more targeted and efficient approach in addressing concerns related to theft or irregularities in power usage among the consumer base.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

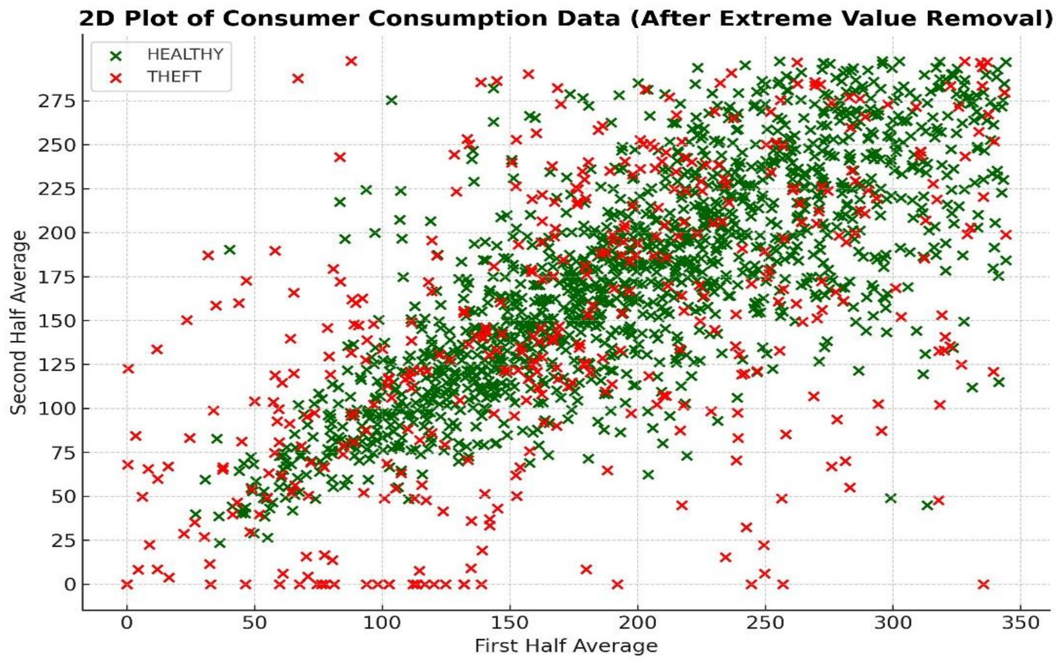

Fig 8(a). shows the minority and majority consumer before sampling

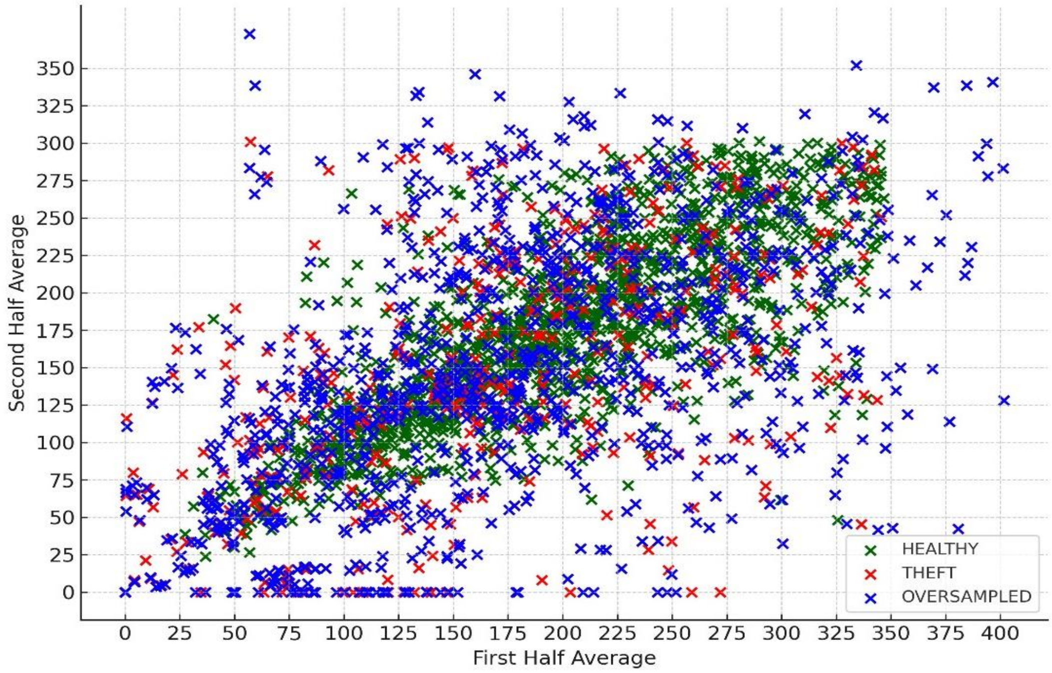

Fig 8(b). shows the minority and majority consumer after sampling

We've employed the SMOTE-ENN data balancing techniques to address the issue of an imbalanced dataset before classifying it using the Extra Tree Classifier. In Figure (a), you can observe that the data class is initially unbalanced. The majority of consumers are represented by green dots, while the minority consumers are indicated by red dots. To ensure that our predictions are accurate and reliable, we took steps to rectify this class imbalance. In Figure (b), you can see that we've increased the number of minority class samples (red dots) by oversampling. This was done to match the quantity of minority consumers with the majority consumers. By doing so, we balanced the dataset, which is essential for achieving dependable results. Without performing this sampling, the results we would obtain are considerably biased and tend to yield unpredictable accuracy. In essence, the classifier's performance before sampling might favor the majority consumers (green dots) due to their numerical dominance, leading to skewed and less reliable predictions. However, after applying the sampling techniques, the classifier can provide more accurate and unbiased results by ensuring that both the

IRJMETS
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

majority and minority classes are adequately represented in the dataset. This, in turn, enhances the model's ability to make fair and precise predictions for all types of consumers.

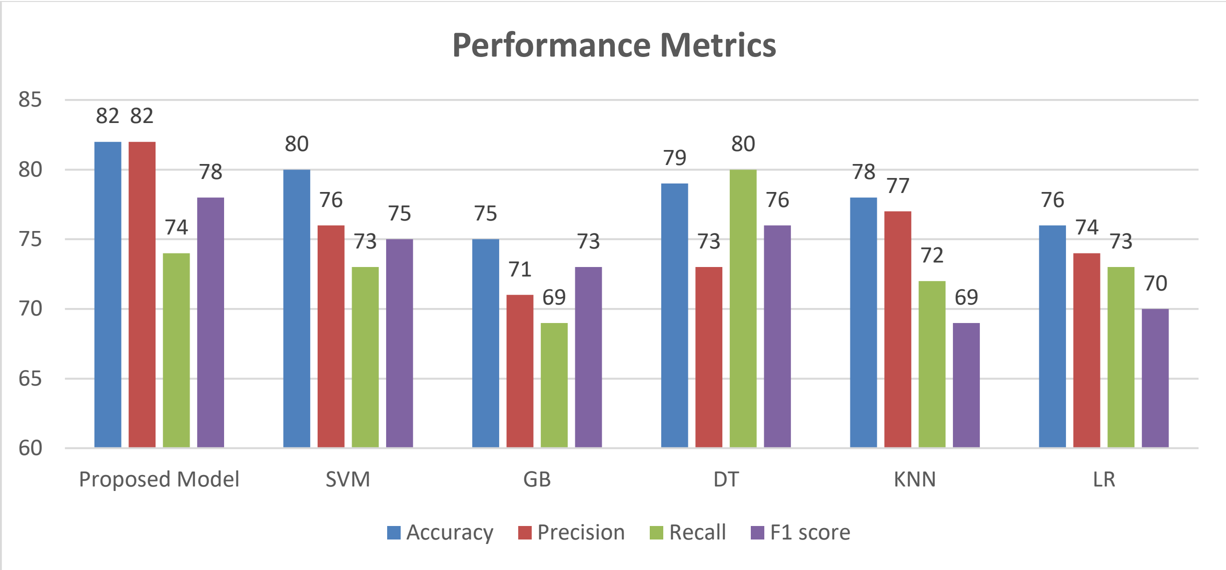

Fig 9: Show chart of different parameters

IV. CONCLUSION

Energy-theft detection is a common and challenging issue in the power utilities. An Efficient Extra Tree Classifier Approach, one of the most effective classifying approaches, , has been used in this study to propose a novel method for non-technical losses NTL identification in power utilities. In order to discriminate between honest and fraudulent customers, the suggested computational model incorporates a variety of distinct variables that were collected from monthly consumer consumption data that was obtained from MEPCO To examine the behavior, more than 2762 customer daily data sets have been trained.

First, during the data pre-processing stage, errors and missing values are handled. The data balancing stage addresses the data class imbalance and balances the class distributions to allow our model to learn effectively. In order to extract and select the features from the collected data set, the SMOTE-ENN technique was used, which over- and under-samples the data classes. Last but not least, the parameters of the employed classifier are examined and optimized during the model training process. The data set was trained using a Extra tree Classifier technique, which correctly categorized the data with a particular accuracy rate. For true positive and true negative outputs, the classifier's precision is 82 while its accuracy is 82%.

The study's main objective is to give power utility companies with comprehensive information and a technical tool for their campaign against electric power theft, one of the major problems in under developed nations. Power utilities need more precise and effective energy theft detection systems, and these classifier techniques will aid in identifying fraudulent customers. In the future, contemporary methodologies will be integrated with decision tree classifier for the detection of non-technical losses with high accuracy.

V. REFERENCES

[1] Bhatti, S. S., Lodhi, M. U. U., ul Haq, S., Gardezi, S. N. M., Javaid, E. M. A., Raza, M. Z., & Lodhi, M. I. U. (2015). Electric power transmission and distribution losses overview and minimization in Pakistan. International Journal of Scientific & Engineering Research, 6(4), 1108-1112.

[2] Jamil, Faisal, and Eatzaz Ahmad. "An empirical study of electricity theft from electricity distribution companies in Pakistan." The Pakistan Development Review (2014): 239-254.

[3] McLaughlin, S.; Holbert, B.; Fawaz, A.; Berthier, R.; Zonouz, S. A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE J. Sel. Areas Commun, 2013, 31, 1319-1330|

[4] Heidari, Mehrdad, Ghodratollah Seifossadat, and Morteza Razaz. "Application of decision tree and discrete wavelet transform for an optimized intelligent-based islanding detection method in

distributed systems with distributed generations." Renewable and sustainable energy reviews 27 (2013): 525-532

[5] Laghari, J. A., et al. "Computational Intelligence based techniques for islanding detection of distributed generation in distribution network: A review." Energy conversion and Management 88 (2014): 139-152.

[6] Nagi, J.; Yap, K.S.; Tiong, S.K.; Ahmed, S.K.; Mohamad, M. Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines. IEEE Trans. Power Deliv. 2009, 25, 1162–1171.

[7] Nizar, A.H.; Dong, Z.Y.; Wang, Y. Power Utility Nontechnical Loss Analysis with Extreme Learning Machine Method. IEEE Trans. Power Syst. 2008, 23, 946–955.

[8] Costa, B. C., Alberto, B. L., Portela, A. M., Maduro, W., & Eler, E. O. (2013). Fraud detection in electric power distribution networks using an ann-based knowledge-discovery process. International Journal of Artificial Intelligence & Applications, 4(6), 17.

[9] Saeed, Muhammad & Mustafa, & Sheikh, & Jumani, Touqeer & Mirjat,. (2019). Ensemble Bagged Tree Based Classification for Reducing Non-Technical Losses in Multan Electric Power Company of Pakistan. Electronics. 8. 860. 10.3390/electronics8080860.

[10] Guerrero, J.I.; Monedero, I.; Biscarri, F.; Biscarri, J.; Millan, R.; Leon, C.; Alonso, J.I.G. Non-Technical Losses Reduction by Improving the Inspections Accuracy in a Power Utility. IEEE Trans. Power Syst. 2018, 33, 1209–1218.

[11] Leite, Jonatas Boas, and José Roberto Sanches Mantovani. "Detecting and locating non-technical losses in modern distribution networks." IEEE Transactions on Smart Grid 9.2 (2016): 1023-1032.

[12] Buzau, M. M., Tejedor-Aguilera, J., Cruz-Romero, P., & Gómez-Expósito, A. (2018). Detection of non-technical losses using smart meter data and supervised learning. IEEE Transactions on Smart Grid, 10(3), 2661-2670.

[13] Tariq, M., & Poor, H. V. (2016). Electricity theft detection and localization in grid-tied micro grids. IEEE Transactions on Smart Grid, 9(3), 1920-1929.

[14] Weckx, S.; Gonzalez, C.; Tant, J.; De Rybel, T.; Driesen, J. Parameter identification of unknown radial grids for theft detection. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Europe Conference, Berlin, Germany, 14–17 October 2012; pp. 1–6

[15] Zheng, Z.; Yang, Y.; Niu, X.; Dai, H.N.; Zhou, Y. Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. IEEE Trans. Ind. Inform. 2018, 14, 1606–1615

[16] Bin-Halabi, A.; Nouh, A.; Abouelela, M. Remote Detection and Identification of Illegal Consumers in Power Grids. IEEE Access 2019, 7, 71529–71540

[17] Kim, J.Y.; Hwang, Y.M.; Sun, Y.G.; Sim, I.; Kim, D.I.; Wang, X. Detection for Non-Technical Loss by Smart Energy Theft with Intermediate Monitor Meter in Smart Grid. IEEE Access 2019, 7, 129043–129053

[18] Gao, Y., Foggo, B., & Yu, N. (2019). A physically inspired data-driven model for electricity theft detection with smart meter data. IEEE Transactions on Industrial Informatics, 15(9), 5076-5088.

[19] Messinis, Georgios & Rigas, Alexandros & Hatziargyriou, Nikos. (2019). A Hybrid Method for Non-Technical Loss Detection in Smart Distribution Grids. IEEE Transactions on Smart Grid. PP. 1-1. 10.1109/TSG.2019.2896381.

[20] P. Massaferro, J. M. D. Martino and A. Fernández, "Fraud Detection in Electric Power Distribution: An Approach That Maximizes the Economic Return," in IEEE Transactions on Power Systems, vol. 35, no. 1, pp. 703-710, Jan. 2020, doi: 10.1109/TPWRS.2019.2928276.

[21] M Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary and E. Serpedin, "PPETD: Privacy-Preserving Electricity Theft Detection Scheme With Load Monitoring and Billing for AMI Networks," in IEEE Access, vol. 7, pp. 96334-96348, 2019, doi: 10.1109/ACCESS.2019.2925322..