ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 8, Issue 8, August 2021

Efficient Power Theft Detection Using Smart Meter Data

[1] Dr. V. S. Bidve, [2] Shreyas Chate, [3] Devyani Jadhav, [4] Shubham Kamble, [5] Krutartha Rasal

[1] Associate Professor, Dept. of Information Technology, MMCOE, Pune, Maharashtra, India
[2][3][4][5] Student, Dept. of Information Technology, MMCOE, Pune, Maharashtra, India

***Abstract*---- Electricity theft is one of the most serious problems for power supplies. Such theft of electricity is productive financial losses to operating companies. It is not possible to detect such theft in person with a large amount of data. Discovering such theft of electricity introduces a robberies' detector (GBTD) based on newer gradient boosting classifiers(GBCs): gradient overgrowth (XGBoost), by categories power boost (Cat Boost), and an easy way to increase gradient (LightGBM). XGBoost learn with one machine an algorithm that offers high accuracy in a short time. In this we are working on the pre operation of the smart meter data at that time includes selection. The actual use of the proposed GBTD for theft recovery by reducing FPR and reducing data storage space and improving the complexity of time for GBTD classifiers receive non-technical (NTL) acquisition.**

***Keywords*— Power Theft Detection, Smart Meter**

I. INTRODUCTION

Many electrical appliances have lost money due to theft of electricity. Here are the different types of electricity power theft, including Touch line or skip power meter According to the investigation [1], 80% of complete burglaries occur in private homes as well 20% in modern businesses and buildings If anyone try get a hand theft so it is unlikely to be large the amount of data will be available. So here this work applying machine learning algorithm to detect theft. Theft can be found by checking for irregularities at user power consumption patterns. From the user basic data is a simple user analysis task behavior. use ML-targeted theft detection model indicating whether an unusual/fraudulent usage pattern has occurred in the SG meter (Smart Grid). Using the height of, a gradient boosting classifier (GBC), more than one ML nontechnical loss (NTL) recovery algorithms.

Existing System

The company employ has to manually check the reading of the smart meter and electricity theft is detected only if the meter is off during the checking. This system is less reliable as most of the time the electricity theft is not detected and output is not accurate. Lot of man power is required with less efficiency of work.

II. MOTIVATION

India loses more money to theft than any other country in the world. The state of Maharashtra which includes India—alone loses $10.2 billion per year, more than all but eight countries in the world. In this proposed system we use dataset having electricity usage of a smart grid (SG) meter (or simply smart meter). Using this dataset, we do feature selection and pre-processing on dataset. When we have large number of features in dataset then feature selection is very important part in our Machine Learning. As we use feature selection it gives us most important feature and this feature selection gives us more accuracy. Then we perform the pre-processing on that data. After that we use the superiority of XGBoost, a gradient boosting classifier (GBC), with Sarimax model over other ML algorithms for nontechnical loss (NTL) detection. Gradient boosting is called gradient boosting because it uses a gradient descent algorithm to minimize loss when adding new trees. This approach supports both regression and classification predictive model. Emphasis was placed on the application of the proposed ML application for theft by reducing FPR and reducing data storage space and improving the complexity of GBTD dividers. Additionally, this suggests an updated version of the six theft cases that exist for real imitation patterns of land theft and apply them to the valuation database of the proposed default algorithm.

III. LITERATURE REVIEW

Researchers have recently used a variety of methods to detect the theft of electricity. These approaches can be divided into three categories: country-based solutions, game theory, and machine to read. Government-based solutions use additional hardware tools such as wireless sensors, distribution transformers, and smart meters to detect electrical theft. This route has high implementation

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 8, Issue 8, August 2021

costs due to the need for additional hardware. In the game talk established method, assuming there is a match between the utility and the thieves. The outcome of the game can be determined by the difference between the use of electricity behaviour of power thieves and harmless users. However, it needs to explain the functionality of the use of all the players in the game, which is really challenging. Mechanical learning methods are widely used of ETD. They can also be categorized by strategies that can be hired (integrated) and monitored techniques (segregation) are later used in labelled data sets to separate fraud and regular consumers. The existing methods used for ETD are presented in Table 1, which contains their offerings and limits. Power theft detection using a device that amplifies the theft detector by feature pre-engineered precision by identifying smart grid power theft, this exposes gradient theft that increases detector (GBTD) based on new gradient consolidation classifiers (GBCs): Gradient Extreme (XGBoost), Increase category (CatBoost), as well how to increase gradient light (LightGBM). While most existing ML algorithms are already focused on fine-tuning the hyper-parameters of classifiers, our ML algorithm, GBTD, focuses on engineering-based performance building to improve the performance of the discovery and the difficulty of time. GBTD promotes both the detection rate (DR) and the FPR standard of those GBCs by produces stochastic features such as standard deviation, mean, minimum, and maximum value of daily electricity consumption. GBTD also reduces the difficulty of classification by factor-value (WFI) extraction techniques.

IV. PROPOSED SYSTEM

The proposed system uses an electronic database smart grid (SG) meter (or simply smart meter). Using this database a selected selections are made as well performing in front of the database. When there are large number of data in the database and the selection of the feature is very limited parofin is important in Machine Learning. As system selecting important feature which gives us more precision and gives preview of that data. After that system uses XGBoost height, gradient upgrades classifier (GBC), in addition to other ML algorithms of non-technical (NTL) acquisition. Gradient consolidation is it is called gradient boosting because it uses a gradient drop algorithm to reduce losses.

System Architecture

The architecture shown in figure 1 of the theft detection system is recommended for actor to detect the irregularities of electricity. Image-based dataset is used for importing image from which number of units are detected, so no human error of manual typing of the consumption units. After that the other features from csv dataset are taken which will be needing to detect the current theft.

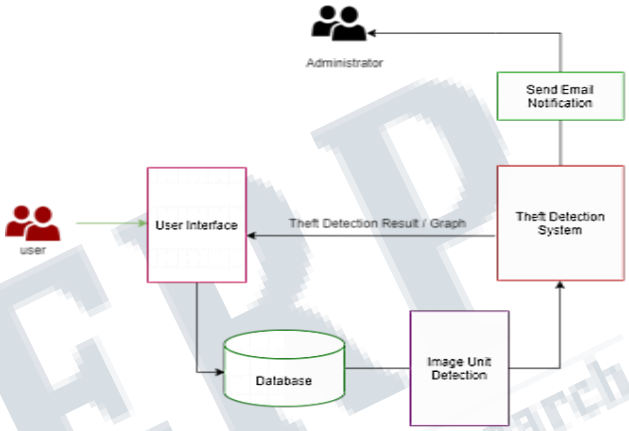

Figure1. System Architecture

The image preprocessing is done and inputs are given to theft detection algorithm which will detect if there are any irregularities in the electricity consumption. An automated system is developed which will then send an alert e-mail to the administrator about theft detection. Google image recognition API is used to identify the number of units from the image. It has pre trained models on large datasets of images and then it classifies the images into thousands of categories to detect objects, places, people and faces in the images and then print the results with the confidence value. This project uses Google Cloud Vision API along with python to detect the number of units from the given image even if the image is blur, is in dark mode, too bright and other such conditions.

SG meter data as input

1. Process the database.
2. Enter the option to select features.
3. Sarimax applied to the data.
4. Theft of electricity is identified.

Software requirement

Operating system : 64-bit Windows 10.
Coding Language : Python
Design constraints : Spyder

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 8, Issue 8, August 2021

Theft Detection Algorithm:

SARIMAX Model: A approach towards regression for creating theft detection work. In an auto regressive (AR) model the model predicts subsequent datum by watching previous data points and employing a mathematical formula almost like rectilinear regression. The auto regressive and moving average models to figure the info must be stationary. This suggests the info must not have trends or seasonality. Integration is taking a difference of the time-series, subtracting the previous value from each value, which tends to form the info more stationary. the moving average a part of ARIMA and SARIMAX. A moving average (MA) model performs calculations supported noise within the data alongside the data's slope. Combining AR and MA alongside differencing (I) creates the ARIMA models. SARIMAX is employed on data sets that have seasonal cycles. The key deduct is that SARIMAX requires not only the p, d, and q arguments that ARIMA requires, but it also requires another set of p, d, and q arguments for the seasonality aspect also as an argument called "s" which is that the periodicity of the data's seasonal cycle.

Automatic Email Notification

Automatic Notification functionality is formed up to send emails if the theft is detected during a meter. During this an email is directly sent to admin if the facility theft is detected using SMTP connection. SMTP connection is encrypted, in order that your message and login credentials aren't easily accessed by others. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are two protocols which will be wont to encrypt an SMTP connection. It's not necessary to use either of those when employing a local debugging server.

V. RESULTS AND EVALUATION

Image Processing:

Image Processing is completed with the assistance of Google Cloud Vision API which accurately gives the right output of the units consumed with none errors. This API from google found to be reliable and faster because it uses pre trained big image datasets to detect the text from image. So, when the image input is captured as shown in figure2, it's seen that exact detection of units was done.

Figure2. Image of Meter Reading

Table1 gives the dataset of the user's vs unit consumption of 12 months, as for detection the algorithm needs previous data of unit.

Table1. Meter Reading Data

1	2	3	4	5	6	7	8	9	10	11	12
116	142	162	185	143	155	148	168	117	137	128	173
261	200	245	254	227	247	232	275	237	272	224	238
333	361	338	389	316	302	371	382	344	324	339	353

As shown in figure3 we can see the output after processing the image which has result text as 530 units. Here Sarimax model forecasted an output of 175.69624 unit which is used to compare with the unit detected in the image and if found in range the theft prediction is done.

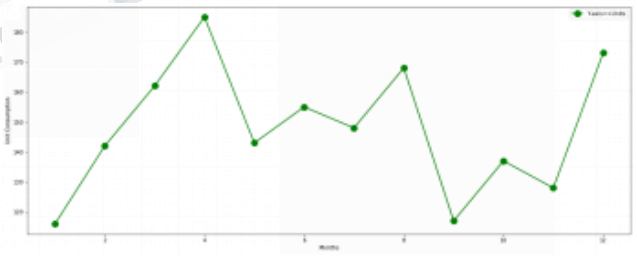

Figure3. Distribution of Readings

From figure3, the difference between the values of forecasted result from Sarimax model and the image processed result text is calculated and then if not found in proper range then the theft is detected. The result can be seen as shown in the figure 4. If the theft is detected the email notification is sent to the administrator of electric utility through SMTP email module, which can be seen in figure 5.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 8, Issue 8, August 2021

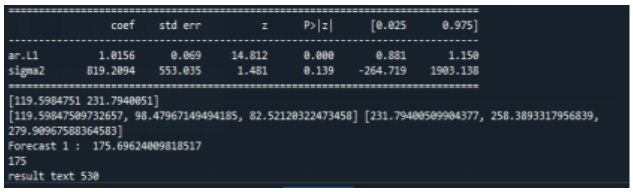

Figure4. Result of theft Detection

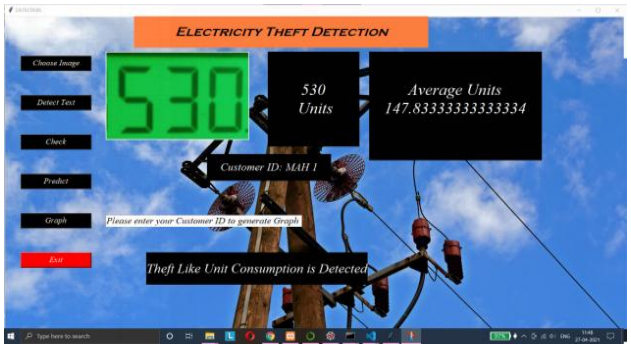

Figure5. Result of theft detection

VI. CONCLUSION & FUTURE WORK

The proposed system detects theft using Sarimax model which gives high accuracy and faster results of genuine consumption of electricity to every user. This system also helps the administrator to get details of theft detected by email so that they can take further actions.

In future The XG Boost model can be applied to generate the forecasts based on the best fit model during hyper parameter tuning. Big Datasets can be used for prediction the electricity theft in the city. More features can be added in this project to show consumption graph to user on front end and also show them range of current range of their genuine consumption.

REFERENCES

[1] 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. 2016.

[2] M. Buzau, J. Aguilera, P. Romero, and A. Expósito, "Detection of Non-Technical Losses Using Smart Meter Data and Supervised Learning," IEEE Trans. Smart Grid, Feb. 2018.

[3] Raghwendra Shukla, Mayur Vidhwani, Prof. V.R. Ghule, "ELECTRICITY THEFT DETECTION USING MACHINE LEARNING", 2012.

[4] Jeyaranjani J, Devaraj D, "Machine Learning Algorithm for Efficient Power Theft Detection using Smart Meter Data," 2013.

[5] S. MCLAUGHLIN , B. HOLBERT, A. FAWAZ, R. BERTHIER, AND S. ZONOUZ , "A multi-sensor energy theft detection framework for advanced metering infrastructures," IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[6] J. I. GUERRERO , C. LEON, I. MONEDERO, F. BISCARRI, AND J. BISCARRI , "Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection." Knowl.- Based Syst., vol. 71, pp. 376–388, 2014.

[7] J. R. FILHO, E. M. GONTIJO, A. C. DELAIBA, E. MAZINA, J. E. CABRAL, AND J. O. P. PINTO, "Fraud Identification in Electricity Company Customers Using Decision Trees," in Proc. of 2004 IEEE International Conference on Systems, Man and Cybernetics, Vol. 4, pp. 3730-3734, Oct. 2004.