International Journal of Multidisciplinary Research And Studies

Available online at https://ijmras.com/

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND STUDIES
ISSN: 2640 7272
Volume:03; Issue:10 (2020)

APPLICATION OF MACHINE LEARNING WITH A REFERENCE TO ELECTRICITY THEFT DETECTION

Chanchala Kumari

M.Phil., Roll No. :140447: Session: 2014-15

University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India

E-mail: chanchalasingh1586@gmail.com

ABSTRACT

That 's important to keep in mind as you go through their pictures. We agree with those observations and propose a change to the six robbery scenarios that would be additional as it should be with reporting close to real-international robbery styles and then practicing them in datasets aimed at realistic assessment and numerical evaluation. We're now using an algorithm that utilizes gadget mastering that will spot the robbery. Checking the power usage pattern of a consumer for irregularities is one way of detecting pilferage by that consumer. An easier way is to evaluate a person's behavior when starting with essential information about the person. We set up a supervised gadget study-based fully theft detection version with the goal of determining whether an unusual or fraudulent use pattern has taken place in a smart grid (SG) meter. For non-technical loss (NTL) detection, we rely on the advantage of XGBoost, a gradient boosting classifier (GBC), over the algorithm that studies discrete devices.

KEYWORDS: Machine Learning, Electricity, robbery styles, detecting pilferage,

INTRODUCTION

A large number of power utilities suffer economic losses due to unauthorized use of electricity. There are many different strategies for stealing electrical power, such as tapping into an existing line or tripping over an electric meter. One survey found that residential homes account for 80% of all international burglaries, while business and commercial locations account for only 20%. If we take some time to detect theft manually, we may not get success as there may be huge amount of records present. We're now using an algorithm that utilizes gadget mastering that will spot the robbery. Checking the power usage pattern of a consumer for irregularities is one way of detecting pilferage by that consumer. An easier

way is to evaluate a person's behavior when starting with essential information about the person. We set up a supervised gadget study-based fully theft detection version with the goal of determining whether an unusual or fraudulent use pattern has taken place in a smart grid (SG) meter. For non-technical loss (NTL) detection, we rely on the advantage of XGBoost, a gradient boosting classifier (GBC), over the algorithm that studies discrete devices. B. The reason for power theft detection equipment is to pick up on suspicious behaviors in the manner in which a smart grid (SG) meter is used to consume electricity (or smart meters at all). Checking a user's power usage patterns for irregularities is one way to detect piracy by that user.

A system of reporting technical knowledge that includes a knowledge acquisition system is built entirely on the fundamental premise of analyzing human behavior based on past facts (ML). This paper details the implementation of a supervised machine learning-primarily piracy detection model that, among other things, determines whether an unusual or fraudulent use sample has been observed in SG. The improvement of a computer model that can quantify robbery frequency has been the subject of investigation in many studies, considering a number of ML strategies. Synthetic Neural Networks, Autoregressive Involuted Moving Common (ARIMA) Time Series Process, and Support Vector Machine (SVM) 9aaf3f374c58e8c9dcdd1ebf10256fa5 are examples of such era that can be found inside the research literature. These days, the authors of confirmed that on the topic of non-technical loss (NTL) detection, the gradient boosting classifier (GBC) known as XGBoost is advanced to various machine learning (ML) algorithms. C. On this paper, we are hoping to provide a comprehensive contrast of the 3 most recent GBCs, which can be Severe Gradient Boosting (XGBoost), Express Boosting (CatBoost), and Light Gradient Boosting Techniques (LightGBM), and We also want to propose a gradient boosting theft detector (GBTD) that is

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

completely based on these GBCs and includes a functional engineering-based preprocessing to enhance the detection rate (DR) as well as enhance the fake fine. is module. D. We are able to ingest a consumer's historical actual usage information in SG for each given consumer fairly quickly. On the other hand, stolen samples may not exist at all or possibly exist very rarely. We manipulate actual use of patrons based solely on mathematical equations in an attempt to compensate for the absence of theft cases within the unique dataset used. The authors of the proposal also note the equations of mathematical piracy, saying that "the motive of piracy is to report consumption less than the fair amount used by the user, or to shift excessive use to a lower-tariff interval".

That 's important to keep in mind as you go through their pictures. We agree with those observations and propose a change to the six robbery scenarios that would be additional as it should be with reporting close to real-international robbery styles and then practicing them in datasets aimed at realistic assessment and numerical evaluation. The detection of suspicious behavior within electricity usage by smart grid (SG) meters is the primary reason for the electricity theft detection process (or smart meters in the true sense). Checking a user's power usage patterns for irregularities is one way to detect theft by that user. An approach to data technocracy that involves knowing the system, with the fundamental premise of analyzing consumer behavior entirely based on predictive record (ML). This paper details the implementation of a fully supervised machine learning theft detection model that, among other things, determines whether an unusual or fraudulent use pattern is visible in the SG. . ML techniques that form a PC version identifying transaction/journal paper training have been a problem to investigate in some papers.

Proposed Energy Theft Detection Machine

In this step, we can discuss the Vigilant Energy Robbery Detection Device from the point of view of its design. Through the use of statistical analysis of records on electricity consumption of both power thieves and normal customers, it can be found that energy thieves' power consumption figures are usually associated with less non-frequent or frequent use than normal. It is elaborated to study the periodicity of energy intake information as it is 1-D time collection data with huge size, energy intake information is often misleading and noisy, and many traditional strategies of record checking, including Contains Synthetic Neural Network (ANN) and Help Vector Machine (SVM), power consumption cannot be eliminated immediately. Nevertheless, it is difficult to see the periodicity of the records in relation to the amount of

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

power used. Consequently, on how to deal with the above difficulties, the CNN technique has been used in this study. For the training of fashion, China's country grid enterprise provided a dataset showing the actual phases of electricity usage.

The dataset includes both normal and fraudulent customers. To begin with , a method of statistical guidance is used to obtain information for training the version. Which will achieve better levels of speed, the preprocessing step routinely involves the creation of artificial data. The recommended model is hyper-tuned in a later step, and finally, the optimized version is checked using test information in the last step. Figure 1 presents an example of the complete system.

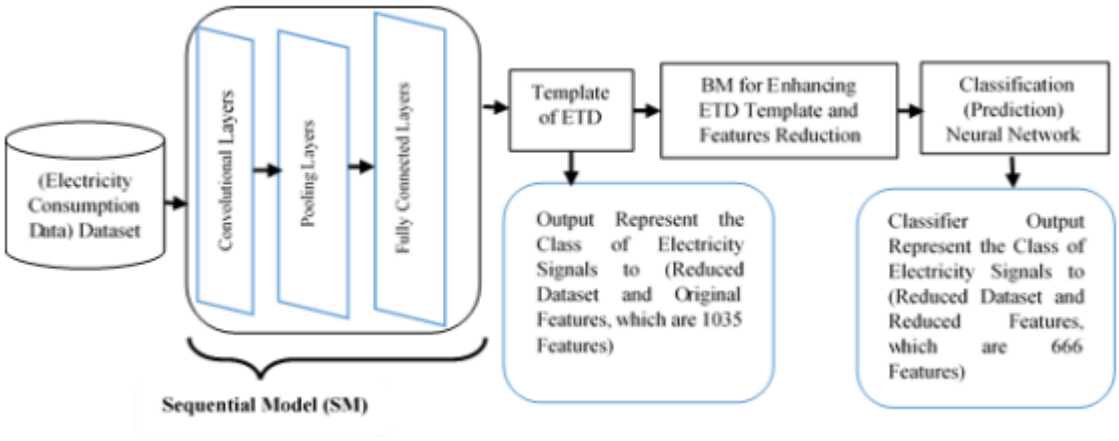


Figure 1.1. Architecture Of The Proposed Model (Cnn And Bm)

POWER CONSUMPTION FIGURES

This unique dataset has a total of , half columns and 42,372 rows. The customers' IDs are indexed in the first column, followed by a link to the predicate labeled "flag" inside the second column, and the time of the week columns start inside the 1/3 column and go all the way through that can be either missing or false called non-numeric (NaN). The fractions shown by means of numbers, some of which are missing or have incorrect values, are the amount of power (power indicator) consumed by each person over a period of years . In addition , there are facts (zero and one) inside the flag column and the entire wide variety (38,757) of zeros in that column. Even though there is only one character represented by the primary inside the "flag" column, t electricity users supplied electricity over a day and a half of electricity usage (from January 1, 2014 to October 31, 2016).

MODIFYING THE DATASET

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

Many different methods are employed for this, making it a good way to drill down to all the ways in which it can be used within construction works . ETD Templates. Those steps are depicted as follows: all zero and nan values in a canonical dataset Generates a new dataset by replacing it with a . 1being taken for; 3) Simplify to a brand new dataset by removing the region and flag columns; Because none of these elements will be used within the device being advised, the reason for this decision is to simplify matters and store time.

CONSTRUCTION OF POWER-THEFT DETECTION VERSION

The ETD technology we use travels several ranges through our machine. The first thing that happened was that we went through different processes to adjust our dataset so that it could be reduced. After that, the Sequential Model (SM) is constructed, a process that can be roughly detailed within the latter component. The introduction of the Prediction Model, also known as the ETD model, is the 0.33 section, and will be considered as one of the methods . The produced SM is used to perform the first operation, and the BM algorithm is used to perform the second operation.

SEQUENTIAL VERSION

The dataset is what the SM algorithm receives as its input, and the reduced dataset is what it produces as its output. The first issue that needs to be achieved in order to make this approach to images well defined is the input size so that it is well compatible with SM. After that, there are two situations in which SM needs to be used: The primary situation involves making predictions about electrical signals through the use of SM's initial fully connected layers. Sending an electrical alert to the SM will accomplish this, and the SM will then return the elegance of the electrical alert sent. The second scenario involves creating a dataset using an array, so that it can be used for training purposes. Furthermore , there are 3 wonderful types of convolutional layers which are 2d (three * 3) in size.

In the last step , the reduced dataset is created with the help of employing the metrics that were generated due to the above mentioned actions. This technique employs three densely interconnected layers, referred to as (Layer 1, Layer 2 and Output).

While a dataset is divided into two parts, the first part of the dataset is used for education and loans for eighty percent of the entire dataset, at the same time the second part of the dataset is used for check outs and bills . Twenty percent of the total dataset. Starting with two layers and

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

moving up to four layers, this technique is used to decide. This layer has a minimum size of 16 nodes and a maximum size of 128 nodes across its various dimensions.

BLUE MONKEY ALGORITHM

As can be seen in Description 2, the BM approach is designed to be a feature if you want to extend the ETD template and provide a back price that specifies the optimal placement. The ETD template is passed into this attribute as its input. The behavior of the BM is simulated with the help of an algorithmic program of the BM. BM is a set of answers to the parent and child, and each bystander and child in the chain has a random set of values. This method inputs a sequence of answers, each of which provides a dataset and a template for reducing the ETD. The output of this set of rules is the reduced dataset and ETD. Each of the 10 solutions had a length of 1035 values, all of which were randomly generated using zeros and ones. The overall range of hired solutions went up to 10. Currently , BM is providing a template which is 1035 items in duration. This countable value can be searched for within the template (zero or 1). This pattern can be used in two steps, specifically: The first aspect that must be performed is editing the dataset so that it is truncated to suit the modified function.

The following step is to assemble a model with an input size that is proportional to the size of the new dataset . The second time this template is used is when there is a new electrical signal that is to be classified. In this example, the template should reduce the values of the power sign using the same method. Therefore, the electrical signal is able to be labeled when using this model.

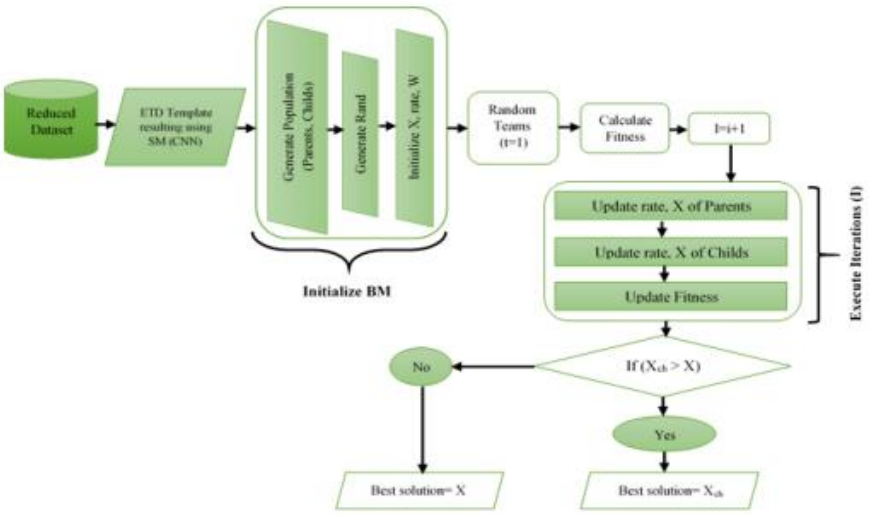


Figure 1. 2. Bm Algorithm

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

DEEP NEURAL NETWORKS

The term "artificial neural network" (ANN) refers to a range of techniques for systems study that have been developed to simulate biological structures found within the human brain. In most cases, they are employed for the purpose of picking out patterns or identifying trends that may be difficult to pick up using conventional gadget learning strategies.

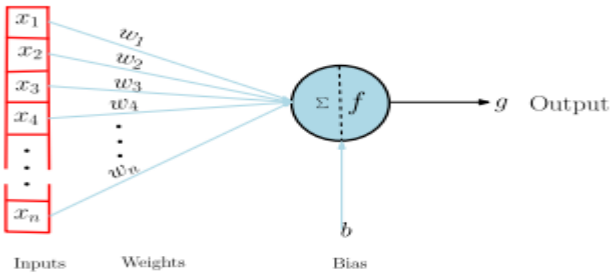


Figure 1.3The First Hidden Layer Neuron Model .

$$g = f(\sum (w_i x_i) + b), \qquad (1)$$

The nodes of a neural network correspond to neurons that are observed in the brain, and the weights connecting the nodes correspond to the connections that exist between neurons. The records that are saved in a neural network are shaped by weights and biases. Studies on artificial neural networks (ANN) are where the concept of deep neural networks (DNN) first emerged.

RESEARCH METHODOLOGY

Big data and data science in the distribution grid

Record technical knowledge can be described as a combination of math, business skills, gear, algorithms and gadget learning strategies. These components work collectively to help localize hidden insights or patterns in the raw facts, which can be a major driving force behind essential enterprise selections. The term "technology" refers to the accumulation of data through methodical research; Therefore, it is possible to interpret technology as a systematic group that accumulates and organizes facts within the shape of observable objectives and predictions. In its most fundamental form, the big data belief record has become more popular among scientists because of the endless value it holds. This is the direction under the condition that the data in the query is understood accurately and effectively. During the past several decades, the world has seen a sharp drop in the cost of storing data, as well as an increase in the amount of information that can be created, uploaded, and analyzed. If you had paid the regular rate for a one megabyte hard disk in 1967, it could have run you a million bucks. That price fell to 500

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

bucks in 1981 and is now less than a cent per gigabyte. This cost reduction is available in light of the fact that it is expected that the entirety of virtual worlds will reach 44 zettabytes by the year 2020. If the calculations are correct, this would mean that there are 40 examples of bytes more than the number of stars that can be found within that part of the universe.

Product support groups and information scientists want to put in extra effort on the way to design and deliver a service or product that is attractive to the target market in today's modern companies, who are realizing that business operations must always be analyzed needs to be done so that the business can operate properly. Growing one 's own operations and offerings is now easier and less expensive than ever before. It is possible to derive a substantial amount of cost from their operating facts. This information has to be continuously analyzed with system mastering algorithms to enhance the effectiveness of their technologies and provide customers with a product that is specifically tailored to their needs. BD has a lot to do in terms of driving corporate efficiencies through improvements in operations and offerings, but there are still a lot of underlying systems and constraints to address over the period. BD also has a lot to offer in terms of normalizing enterprise performance. For example, with the help of BD Insights, companies are able to realize the warning signs that may stand out for the duration of the recruitment system and choose the people who are most likely to meet all the job criteria. Huh. Because a set of rules predicts the right candidate more than anyone can guess, many companies in the modern world were forced to lay off most of the people in their human resources managers. This capacity is eliminated in the form of a reduction in costs associated with both the education of personnel and the search for new ones. The onboarding segment is a great area to start looking for potential problems, and advanced analytics for human resources can help with tracking employee retention overall.

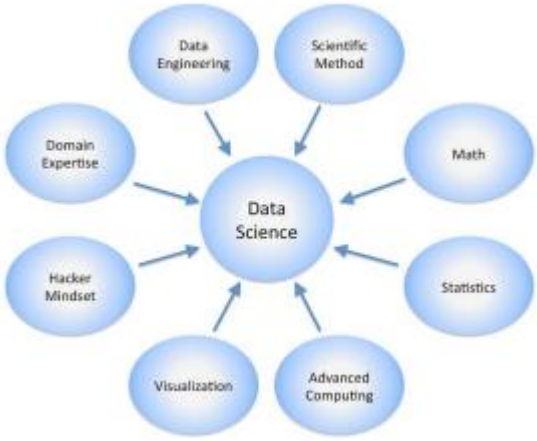


Figure 1.4 1of Data Science

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

Furthermore, BD can help enhance the operationalization of many socio-technical challenges by incorporating its analytical features. Those demanding conditions include sustainable urban planning and IoT technologies to control waste, parking and energy intake. Other challenges include reducing pollutants and costs, as well as improving the pleasantness of existence. The list should go on, but the point is that BD is most effectively going to beautify its role in areas such as environmental renewal, public health, poverty reduction, and many other public sectors. Satellite images, advanced statistics processing, and the involvement of a vast range of humans are examples of progressive processes that are reshaping the way things are accomplished to avoid deforestation. Endangered species conservation and poaching prevention each use similar collections of geo gear for you to benefit from a perspective on how to preserve nature on a micro level while exploring on a macro level. With the help of BD, medical facilities are able to decipher total DNA collections in a matter of hours, increasing their ability to screen premature and sick babies in addition to becoming aware of patterns in diseases and potential mutations. To analyze their every breath and heartbeat. The amount of data that scientific professionals will be able to collect and compare is projected to increase due to increased use of wearable technologies consisting of health bands and smartwatches. An entirely new medical paradigm, known as fact-intensive medical search (DISD), has emerged because of all the potential and truly valuable qualities that may be buried in records. Grand statistics challenges fall under this category. scope , there are also algorithms at times that are done for artificial intelligence. Because of this , the firm is able to offer in-depth insight and improve the performance with which wind farms are run.

DATA ANALYSIS

Intelligent Approach to Management of NTL and Synthetic Profile Modeling

Threat model

The term "chance variant" often refers to a selective attack on the gadget, suggesting the presence of various attack vectors. For example, a scheme a fraudster chooses to reduce or completely inflate his invoices, as well as well-known gadget vulnerabilities, are examples of attack vectors. Threat variant estimation is a technique that can be used to select other styles of NTL. The main feature of hazmat fashion is to mark any discrepancy in intake styles. Various

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

NTL can be identified using this method . According to , energy fraud can be divided into the following three categories:

Cyber-attacks: Gaining unauthorized access to a smart meter, including hijacking a verbal exchange community and tampering with a smart meter garage; May appear at the smart meter level in addition to the utility communication network;

Physical attacks include bypassing the meter, tampering with the meter so as to detect low usage, tapping (hooking) on low-voltage cables, and similar games. It is not uncommon training to use equipment, such as powerful magnets, for you to intervene. At different times, the meters would be scaled back or perhaps unplugged entirely. Connecting a network of high consuming equipment or home appliances to external feeders is an example of a type of fraud that is gaining reputation and can be seen in all international locations regardless of their socio-economic prominence. This type of fraud makes another customer liable for the invoice, which is usually an agency or community building. In recent years, while bitcoin mining has gained a lot of fanfare and supported a spike of illegal meter connections, this type of robbery has seen a particularly strong reinforcement, leading to an increase in thefts of various kinds.

Numerical evaluation using initial load profile

The organizations ultimate aim is to establish a unified electricity market for Europeans so that it can more successfully meet the needs of customers located at some level in Europe. The Smart Metering Project was conceptualized in 2007 with the aim of conducting a cost-benefit analysis for a nation-wide deployment strategy, analyzing how smart meters impact consumer behavior, and finding out whether modern smart meters How good is the infrastructure? plays. More than 5,000 households and small to medium-sized commercial enterprises make up the customer dataset, and the PAIN was conducted between 2009 and 2010. To participate in the tests, households and companies were also asked to complete surveys that specified certain usage and relationships between elements that included demographics, scale of furnishings, way of life, and so forth. Of course, the information given is anonymized if you wish to meet the privacy issues of the utility users and encourage the expanded study and development of new goods and services within the destination.

All facts it provided include a summary of intake information presented in a format that is every 1/2 hour in addition to documentation, a pre- and post-trial survey questionnaire for both households and groups, and a document with findings. of testing. The dataset containing the weekly usage patterns of three hundred consumers has been randomly selected for the

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

reason of this thesis. This dataset also includes a half-hourly live consumption file for each buyer , measured in kWh. The date range from July 14 to July 19, 2009 has been set as the weekly deadline. Given that the intake data used in detecting NTLs are routinely unbalanced, it is decided to synthetically generate 2 robbery profiles in sets of 300 . The amount of information is considered sufficient in order to make a selected comparative evaluation between exceptional methods . Because the dataset is sampled at a typical half-hourly interval, we are able to characterize the intake of our customers every day using a vector of 48 features, each of which has been studied in one of these periods. is shown through. Description 8 shows the daily intake behavior of a patron who was randomly selected.

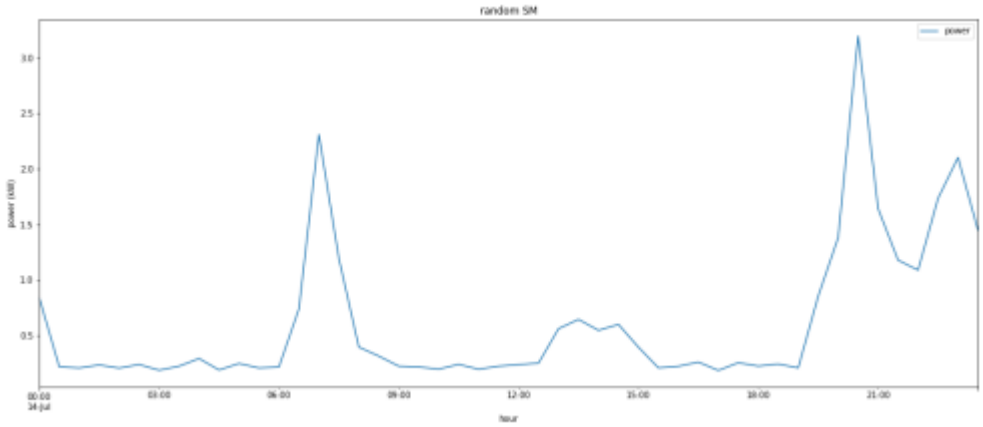


Figure1.5 : One day record of consumption of a random customer.

Creation of new theft cases

The theft incident was followed as it was presented at trial because it reflects a type of fraud in which the offender reports loads almost continuously throughout the day, every day. For the purpose of this thesis, the synthetic tortuous profile is produced through the calculation of the average normal of actual consumption curves that were uniformly distributed with little variation among historical information over recorded time periods so that This may help to get an accurate picture of the gadget. Probability. This is accomplished by allowing you to achieve the intent of creating an artificial cheating profile that matches this thesis. Inside the real world, this form of reading manipulation is done in an attempt to register some usage and to support irregular, stand-by consumption, including what can be expected in a rural home at some point. Working week, eg. Theft pattern was reshaped to create a higher top limit as it is very important to note that the incidence of theft may not be frequent; A constrained reporting of "fraud" would likely arise in conjunction with some form of intake price manipulation. That 's why a pretty high restriction gets set up. Therefore, a randomizer feature was used to generate the factor of multiplication, and it was set so that it fell anywhere between zero.1 and 1.0. To validate the

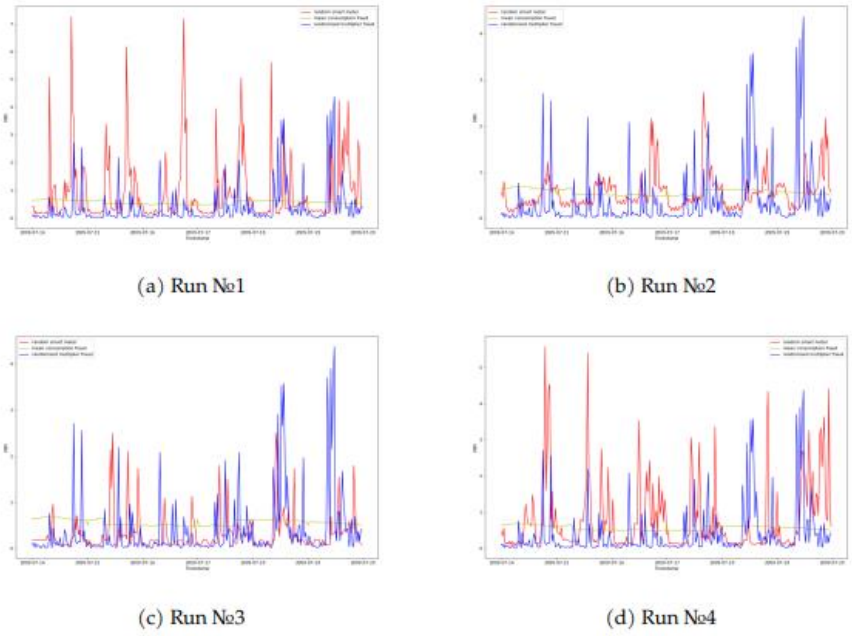
Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

efficacy of an unsupervised classifier set of rules, the plan is to first fabricate fraud examples that have characteristics that are similar to actual theft, followed by labeling fraudulent entries in the database. Given the values of their usage statistics, it is reasonable to assume that both scammers are residential customers. If xt is the actual intake charge set in the dataset, the cheating styles obtained can be written as:

$$t1(xt) = xt * rt(rt = random(0.1, 1.0));$$

$$t2(xt) = mean(x)$$

Illustration 9 depicts the intake patterns of two dishonest customers generated using actual consumption data from customers who were presumably honest. This sample is mixed with a random actual consumption profile to provide a visual representation of the viable diploma of fraud. Instead of finding a day-to-day load profile for this contrast, a 6-day profile was looked at in order to get a better sense of the periodicity of the facts. After going over the plot several times, it becomes clear that the dataset created includes both residential and industrial customers. As a result, some comparisons appear to have a substantial difference in usage, while others are remarkably similar to the deceptive state. A randomly chosen meter is indicated by a red line.



(a) Run №1 (b) Run №2

(c) Run №3 (d) Run №4

Figure 1.6 plot comparisons

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

Similar to the number one dataset that was generated researching 300 clients over the course of six days , additional datasets were compiled using applicable information from the primary readings, each of which included an effect of forty-eight half of the newly produced datasets. Has- Hourly recordings every day over the course of 3 weeks for 2 customers who were owed money were tampered with to appear fake. Although the dates for when actual consumption was adjusted to convert to fraud varied, fraud remained the same for the duration of the sample development process. These datasets were advanced with the aim of demonstrating a clear assessment of the behavior of clustering algorithms over an extended period of time.

CONCLUSION

objective, the interpretation of ultramodern images can be done in a variety of state-of-the-art approaches, however the result that has been anticipated has been achieved: a clever machine has been proposed that allows intake sampling Identifying non-technical pitfalls for the purpose of detecting today's clustering techniques through software. It was possible to evaluate the overall performance that was implemented and was in line with the main objective, which in all likelihood was the modern detection of fraudulent consumption trends that, in the latter instance, were real -world scenarios. In, the workers will be inspected through the application body. This assessment was done by comparing the results of several approaches used today.

REFERENCE

1. C Andrews. [online]. Available: http://creativecommons.org/licenses/by-sa/3.0
2. H. T. , Bei Zhang, Y., "Big Data Analytics in Smart Grids: A Review," Energy Information, Vol. 1, pp. 3–4, 2018. [Online]. Available: https://energyinformatics.springeropen. com/articles/10.1186/s42162-018-0007-5
3. Xantacross. [online]. Available: https://commons.wikimedia.org/wiki/File:Euclidean_vs_DTW.jpg
4. A. Mamer and K. Benhamad, "Machine learning techniques for energy theft detection in AMI." New York, NY, USA: Computing Machinery Association, 2018. [online]. Available: https://doi.org/10.1145/3178461.3178484
5. P.-N. Tan, M. Steinbach, and V. Kumar, Introduction to Data Mining. Addison Wesley, May 2005.

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*

6. KMU Ghori, M. Imran, A. Nawaz, RA Abbasi, A. Ullah, and L. Sajathmari, "Performance Analysis of a Machine Learning Classifier for Non-Technical Loss Detection," J Ambient Intl Human Comput, 2020.
7. I. Breedo, V. Kaverin, D. Abisheva, and A. Kolychev, "Monitoring of leakage currents of suspension insulators of high voltage overhead power lines."
8. J. Parmar, "Total Losses in Power Distribution and Transmission Lines: EEP," December 2017. [online]. Available at: https://electrical-engineering-portal.com/ Total-losses-in-power-distribution-and-transmission-lines-1
9. J. Navani, N. Sharma, and S. Sapra, "Technical and Non-Technical Losses in Power System and Its Economic," 2012.
10. S. Amin, GA Schwartz, AA Cardenas, and SS Shastri, "Game-theoretic model of power theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure," IEEE Control Systems Magazine, vol. 35, no. 1, pp. 66–81, 2015.
11. Northeast Group, LLC, "Power Theft and Nontechnical Losses: Global Markets, Solutions and Vendors," 2017.
12. L. Arango, E. Deccache, B. Bonatto, H. Arango, and E. Pamplona, "Study of the impact of electricity theft on the economy of a regulated electricity company," Journal of Control, Automation and Electrical Systems, vol. 28, June 2017.
13. F. Jameel and E. Ahmed, "An Empirical Study of Electricity Theft from Electricity Distribution Companies in Pakistan," Pakistan Development Review, Vol. 53, no. 3, pp. 239–254, 2014.
14. T. Smith, "Electricity Theft: A Comparative Analysis," Energy Policy, Vol. 32, pp. 2067–2076, February 2004.
15. P. Conceicao, "Human Development Report (2019): Beyond income, beyond average, beyond today: Inequalities in human development in the 21st century," 2019.

Chanchala Kumari*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: chanchalasingh1586@gmail.com.*