

# Artificial intelligence for energy fraud detection: a review

Sushmita Poudel, Udaya Raj Dhungana

Department of Electrical and Electronics Engineering, School of Engineering, Pokhara University, Pokhara, Nepal

---

## Article Info

### Article history:

Received Nov 27, 2021

Revised Feb 28, 2022

Accepted Mar 19, 2022

---

### Keywords:

Artificial Intelligence

Electric utility

Energy fraud

Non-technical loss

---

## ABSTRACT

Energy fraud in the distribution sector of electric utility includes electricity theft, meter tampering, or billing error. This fraud causing non-technical loss has led to an economic loss of the company. In order to detect and minimize fraud, different technologies have been used. From conventional methods to development in the field of artificial intelligence (AI), effective and reliable fraud detection methods have been proposed. This paper first provides an overview of different proposed methods for non-technical loss detection and evaluate the advantage and limitation of using those methods. Furthermore, several supervised and unsupervised machine learning methods for detecting electricity theft are discussed in summary along with their metrics and attributes used. Finally, these methods are classified based on the overall operation and the parameters used. This paper provides comparisons of several fraud detection methods using AI along with their weak and strong points and this information is very useful for the researchers who are working in the field of AI method for detecting fraud.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



---

## Corresponding Author:

Udaya Raj Dhungana

Department of Electrical and Electronics Engineering, School of Engineering, Pokhara University

Dhungepatan, Pokhara-30, Kaski, Nepal

Email: udaya@pu.edu.np

---

## 1. INTRODUCTION

In the power grids, losses of electrical energy in the transmission and distribution level include both technical losses (TLs) and non-technical losses (NTLs) [1]. These losses come at a very high cost to electric power companies. TLs are unavoidable loss that occurs naturally in the system. They are caused due to the dissipation of electricity in the power lines and equipment which are used for the production, transportation and distribution of electricity. So TLs involve substation, transformer and line-related losses like copper loss, dielectric loss, losses due to overloading and improper earthing [2].

Since TLs depend on the quantities of the load in the power system so they can be easily computed and controlled by developing smart infrastructure and devices. NTLs, on the other hand, is the loss of energy that is delivered but has not been billed. NTLs occurs probably as consequence of electricity theft and meter inaccuracies. Therefore NTLs are also termed as administrative losses (commercial losses) [3]. The basic causes of NTLs are: i) low-quality infrastructure; ii) illegal usage of electricity; iii) lower consumption by tampering of meters; iv) energy meter error; v) tapping low tension lines; and vi) unpaid bills and delayed meter reading.

So the total loss in a power system is the sum of technical and non-technical loss. The important task for a power sector is to minimize these losses occurring in a power system by detecting the loss before the case becomes worse. Mainly the loss which is difficult to calculate and detect need to be firstly addressed i.e, NTLs. There are various activities occurring outside a power system whose actions can cause loss of electricity

leading to power shortage. Such a loss of power caused by external action in a power system is non-technical loss [2]. NTLs are difficult to detect and measure because their computation requires the preliminary data to be evaluated. In order to determine NTLs, TL is evaluated and subtracted from total loss to give the computed result as NTL. NTLs mainly relate to energy theft in one way or another. It involves the unmanageable customer process containing multiple factors causing fraud to the electric utility [2] and such a crime is defined as energy fraud.

Basically, energy fraud is the crime committed when a person has manipulated their meters in order to pay less or not pay at all. The fraud is usually done by tampering the wires and connectors so that the meter no longer will record the energy units efficiently and correctly which eventually leads to cheaper bills. Essentially, electricity theft involves the process of manipulating the meters to get electricity for free. The NTL due to energy fraud has become a huge issue in the countries like Brazil, India, Nigeria, Pakistan, etc. almost across the world and particularly in the energy market sector where it often ranges up to 40% of the total electricity distributed [4]. NTL has resulted loss of profit in the energy sector. It causes a significant loss in electricity distribution companies either of developed, under-developing or developing countries. Along with the economic loss of the country, the fraud done in the energy sector can become life threatening issue. People's safety is in danger while attempting fraudulent behavior. A person attempting for such activity of electricity theft could get injuries due to a short circuit further leading to shock, fire and explosions. Proper system security and formulating a different method for the identification of such losses has become an important concern for attenuating the losses in the power sector. Many research has been done for identifying the various factors which cause NTLs and how these losses can be detected. For the detection of NTLs various traditional and machine learning (ML) methods are used [5]. The traditional method like an on-site inspection by trained technicians are prevalent in many countries. In this process of detection method, the consumer having a high deviation in energy consumption pattern is taken under inspection. The energy consumption deviation pattern for a particular month and that of its previous month or particular month deviation pattern to that of the same month in the previous year is analyzed by the field staff. If the deviated amount is unusual the consumer is suspected of causing fraudulent activity. Since there are a large amount of the consumers on distribution network whose energy consumption deviation is to be analyzed, the method can be too complex and strenuous. Also, there are various factors which can significantly cause an increase or decrease in energy consumption patterns such as weather, tariff, vacations, smart meter data, consumer type (industrial, commercial, domestic). So the traditional methods for detecting a fraud in energy consumption are considered less effective and more time consuming methods. These conventional methods eventually lose their place in the modern era of the power system.

An effective method for reducing the NTLs in the electricity distribution systems is to replace the conventional methods with ML algorithms. Using ML algorithm one can learn from the previous data. A fraudulent activity has specific features which are causing it to become fraud and different than the non-fraud. By analyzing these tons of features, ML algorithm is used to detect the stealthy fraudulent pattern which is causing unusual deviation in energy consumption and recognize them further. With the knowledge of the data pattern, the electricity consumption can be identified in a detailed way in some events related to the quality of electricity or unauthorized interventions in electrical installations [6]. Different researchers have proposed a new and more efficient methods for detecting electricity theft. With the development in the field of AI, the detection methods have also become advanced compared to a conventional method. AI detection method is considered superior in terms of accuracy, efficiency, time-consumption, precision, and labor required [7]. There is a growing number of researches been done for NTL detection using AI techniques.

Despite the trend towards the development of AI based detection methods, there is a lack of one complete source of information for studying AI based NTL detection methods. The objective of carrying out this comprehensive review is to study and classify various AI-based electricity theft detection methods. The methods are compared regarding the features of attributes, algorithms and performance metrics applied. Different ML methods which have been used in the field of electricity theft are discussed in the summary. The benefits and limitations of using every detection method are further discussed for providing comparative information to new researchers working in the field of NTL detection. The primary contribution of this paper is to present a comprehensive top-down approach for reviewing AI based NTL detection methodology. The objectives of the paper include: i) Review on the various sources from where the data are collected which are used for NTL detection; ii) Review on the various attribute's features used in each method; iii) Review on available AI methods for detecting NTL; iv) Review on the performance metrics used in each learning method;

and v) The detailed comparison of all these methods including their advantages and limitations.

In order for achieving the objectives of the current review, an analysis of major articles related to NTL detection method using AI techniques has been carried out. The selected articles reflecting the detection of energy fraud using AI technology are thoroughly reviewed and analyzed. The paper is organized as follows: i) Section 2.1 provides a description of NTL data sources and various attributes used for detecting NTLs; ii) Section 2.2 and 2.3 set out a description of AI based NTL detection method; and iii) Section 2.4 provides a description of the performance metric used by ML algorithms for fraud detection. The comparative study of reviewed energy fraud detection method are set out in section 3.

## 2. METHODOLOGY

Many research has been done for efficiently identifying fraudster customers in the energy sector. Basically, the ML and AI algorithms used for identifying and solving various anomalies include different methodologies like 'supervised' and 'unsupervised' learning. But before the learning methodologies are formulated, it is imperative to introduce various sectors from which the data have been collected to derive computational intelligence and extract the important features from those data. In summary, the first step of the methodology involves cleaning and integrating the database achieved from various data sources, the second step is to select key attributes for the model and the further step is to feed the features of those attributes of the indicated learning models. These general steps are illustrated in Figure 1 and described accordingly in further sections.

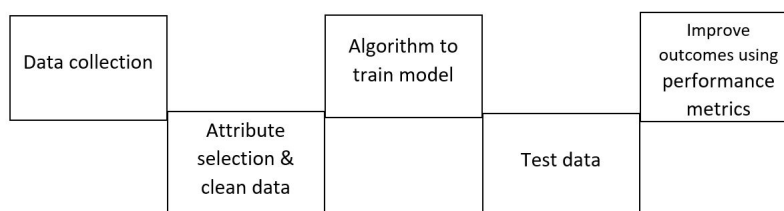


Figure 1. General Steps of Building AI System

### 2.1. Data collection and attribute selection

The time-series energy usage data are collected from various energy sectors. The collected data are used for extracting different features of the customer. The information extracted from datasets plays an important role in AI method for training the datasets or for relating real-time scenarios. In detecting NTLs, the foremost data to be studied includes an energy consumption pattern of selected consumers or a specified location. For example, the energy consumption dataset of various homes in the USA for the study was taken in [8]. The datasets contained aggregated electric consumption data of homes with respect to date and time. Here the average number of persons in each house has been taken because the dataset did not contain detailed information on the number of persons in each house. Whereas the datasets can also be extracted from smart meters. The dataset consisting approximately 5,000 residential households and 600 businesses consumption data were taken from smart meters by [1]. This data was given by the Irish Social Science Data Archive Center of almost two years (2009-2011) and from which every 30 minutes data were captured for study. The consumer may belong to any category of energy consumption like industrial, and commercial. In which category does the consumer belongs to can be one of the major cause for change in consumption pattern. It is necessary for classifying consumer profiles. So the dataset was classified as industrial profiles and commercial profiles with a number of 5190 and 8067 consumers respectively in [9]. The labeling of the datasets was performed by technicians of the aforementioned company. The datasets were obtained from a Brazilian electric power company. Similarly, the real data of more than seven million consumers were taken again from a Brazilian electric power distribution company for the study done by [10].

Quality data are of importance for any machine learning model to work efficiently [11]. Also for performing various actions, firstly training datasets must be fed into the machine learning algorithm, followed by validation datasets (or testing datasets) which ensures the model is interpreting the data accurately. The more data you provide to the ML system, the faster that model can learn and improve. Different research

studies have used different types and numbers of datasets sharing common attributes for detecting fraud in energy consumption. Among the considered attributes for each consumer, there are those whose values change with time known as dynamic variables and the ones that are kept constantly unaltered with time called static variables. The dynamic variables are the important factor to be taken into account for fraud detection because they represent the behavior of the consumer on time domain, i.e, for each time unit considered, there are different new values, so the dynamic variables are more complex to be handled and analyzed.

In mining process the customers are chosen based on the time period of recorded invoices, geographic area, contractual power, consumption range, history of customer inspection and then pre-processing of data is done. The data were pre-analysed by eliminating customer who has less than six month register per year and also customers who had negative values on consumption attributes in [12]. The customers with very low consumption are suspected and customers with a yearly consumption below 100 kWh customers and with a high consumption of reactive energy regarding active energy consumption is kept under inspection. Each consumer smart meter data were taken by [1]. From meter id the consumption data in kilowatts-per-hours (kw/h) for a particular date and time of each household were taken as a key feature for defining the pattern of energy consumption. Pre-processing of the data was done by searching the missing values and replacing them by average energy consumption of that particular day. The second step of cleaning the data involves identifying and eliminating outliers such as peak energy consumption during special occasions, holidays, celebrations which are not assumed to be considered fraud. Lastly, the parameter 'month' is not given concentration as it did not show any major significant changes in the result. So data cleaning and feature selection are done for simplicity. Likewise, in an initial stage seven data of consumers were taken into consideration by [10] which includes consumer database and their socio-economic features, consumption history, inspection history, services requested history, history of ownership exchanges, queries debits history and history of meter reading. These data were integrated using a unique key known as consumer installation code. So that if any incorrect or duplicate records were found they could be removed easily using the code. Further, a single database, including all the seven attributes were generated. The single database was used as input to feed the data mining algorithm in the paper.

Basically, in many of the papers reviewed, once trained and classified sets of attributes were fed into the system, then subsequent datasets were used to sculpt the ML model going forward. Some key attributes used as input in considering papers are mentioned in Table 1.

Table 1. Different attributes used

Attribute selected	References
consumer Id., electric demand, consumption(kwh)	[3]
maximum demand, load factor, installed power	[9]
geographical area, consumption range, history of inspection	[12]
economic sector, billing frequency	[13]
location, metering type, no of phase	[10]
meter id, date and time	[1]
tarif category(residential, commercial), mean consumption	[14]
no.of appliances, temperature,season	[8]
smart meter , old fraud ( yes or no )	[15]
average voltage, power factor, time-stamp	[16]

## 2.2. Supervised machine learning methods

Supervised machine learning methods used for detecting the fraud in the energy sector utilize the data of both fraud and non-fraud for training the classifier. The supervised method for fraud detection uses labeled datasets while training algorithm. The datasets can be later tested on new datasets. This method studies the patterns of a consumer of their data on energy consumption for prediction purposes [17]. But when labeled data of fraudster consumers are not available or when the number of fraud cases is much lower than those of non-fraud, supervised methods are difficult to use. The supervised machine learning techniques that have been used to solve the NTL detection problem are depicted in Figure 2.

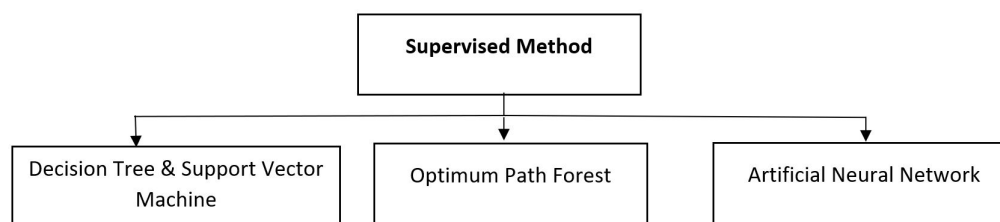


Figure 2. Supervised Machine Learning Method for NTL detection

### 2.2.1. Decision tree and support vector machine

Support vector machine (SVM) is a supervised machine learning technique used for the classification of data. SVM classifies the unseen data by reducing classification error. Whereas, decision tree (DT) is the classification technique that divides attributes into classes according to their features. Jindal *et al.* proposed a top-down approach based on both the method (DT and SVM) to detect the theft in complex power network [8]. Using this scheme the theft was detected precisely in every level of power transmission and distribution where real-time electricity theft was located. DT was trained to detect theft by calculating the unexpected electricity usage of the consumer. After the data was collected in the utility server, the total power transmitted and received was compared and computation was formulated. If the transmitted power was more than the received power including the losses in transmission and distribution, the consumer was manually inspected else the process was repeated for another level. Here in the paper, both DT and SVM methods were used for detecting the fault caused in both the transmission and distribution sectors. Different parameters are computed in DT and then SVM operates comparing those computed values with the actual energy consumption and therefore finally classifies consumers as normal or malicious.

### 2.2.2. Artificial neural network

Artificial neural network (ANN) is a machine learning method consisting of a number of neurons numbered 'N' and models an architecture so known as multilayered machine learning algorithms. The number of inputs is taken as a neuron and an activation function is applied to this input, which results in the activation level of neurons. Knowledge about learning tasks is given in the form of an example called training example. So an ANN can be simply classified into a neuron model which is an information processing unit, an architecture that include a set of neurons, their links and a learning algorithm used for training the datasets. The ANN technique is used for fraud detection due to its noise robustness and fast response qualities. An approach of machine learning technique i.e ANN has been applied for reporting energy fraud and have used smart meter for analyzing the data of energy consumption in [1]. The two main procedures for pre-processing the raw energy consumption data before they are analyzed were data cleaning and feature selection. The main goal of this paper was to learn the consumption behavior per consumer and predict future energy consumption measurements. The number of consecutive days 'N' served as the input layer attribute of the neural network. Total no of  $48 \times N$  nodes i.e, each day containing 48 measurements were taken. For simplicity, only one layer of the node was taken which was a hidden layer and can be easily adjusted. There was only one attribute at the output layer which represents the expected value in smart meter reading data series following the consecutive data points.

Similarly, the use of knowledge discovery can also be utilized for classifying the consumers to be inspected [10]. Here, ANN was used in the data mining process to train and classify the datasets. After defining the architecture, k-fold cross validation method was used to code the data mining where  $k = 10$  i.e., out of 10 subsets nine of them were used for training the data and one is used to test the model. The cross-validation process was used in this scenario to ensure that the model has good generalization ability.

### 2.2.3. Optimum path forest (OPF)

Optimum path forest (OPF) is also a supervised machine learning graph-based algorithm that is usually used for classification applications. The classification process in OPF comprises two steps, i.e., fit and predict. Moreover, the use of the pruning algorithm like OPF can detect the similar type of samples from training data sets and remove them from the process of classification. Likewise, an experiment has concluded that

such removal can prune up to 50 percent of the original training set without affecting the accuracy of the test set and can even improve it [9]. Since this is directly proportional to the number of samples in the training set using OPF pruning algorithm, the test phase of the OPF-based classifier can be sped up.

### 2.3. Unsupervised machine learning method

The method that does not require any data that is already labeled either negative or positive to train the classifier is known as unsupervised methods [18]. These methods do not need supervision. The model work on its own to get the hidden information from the data provided. As compared to the supervised machine learning algorithms, unsupervised methods can perform more complicated processing tasks. For the NTL detection problem, various unsupervised machine learning algorithms which have been used is depicted in Figure 3.

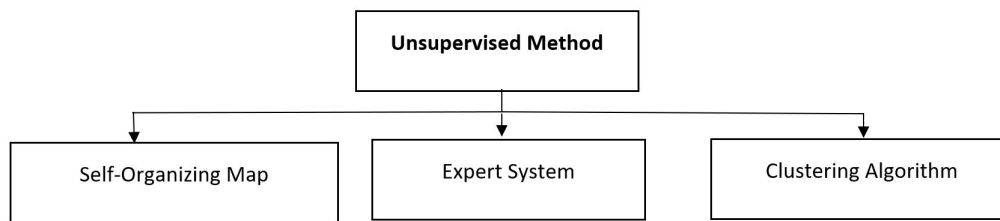


Figure 3. Unsupervised Machine Learning Method for NTL detection

#### 2.3.1. Self-organizing map

Self-organizing map (SOM) is a specific ANN model of non-supervised knowledge working on two modes i.e., training and mapping. Training will build the map using data sets and mapping classifies new available inputs automatically. Cabral *et al.* [3] applied SOM for detecting energy fraud. SOM, here operates by comparing history behavior of consumer consumption data and compared with present measurements. The researchers have mainly focused on consumer consuming high voltage electricity. The data were taken from the Brazilian electrical energy distribution company. The database contained weekly aggregated consumer energy consumption entries. Several consumers were selected for simulating fraud, an intentional drop of 30 percent on their energy consumption. The researchers reported, in 85 percent of cases, the system could identify 30 percent drop in consumer energy consumption behavior and raised an alarm.

#### 2.3.2. Clustering algorithm

Clustering is mostly done in the initial stage for pre-processing data. Normally it is used for detection of anomalous behavior. It will assemble similar type of the consumers which have different energy consumption patterns and then a classifier will be trained on them to identify or classify the unable data. Further, uses the information obtained for pointing out any anomalous for new data available. This process increases the classification performance by reducing false positive cases. Clustering algorithms are used several times for detecting NTLs [19],[20]. It is not ideal for all types of problems, but combining the clustering technique with other data extraction methods can help to solve complex problems.

#### 2.3.3. Expert system

Expert system in AI is used for enhancing decision-making ability of human experts. So expert system is based on the instruction given by the professionals. They are used in both supervised and unsupervised methods. In NTLs detection expert system is modeled as per the instruction given by human experts based on the requirements. León *et al.* [13] proposed a paper where an integrated expert system (IES) was used for analysis and classification of all the available information of customer which are useful for detecting fraud in a system. The data were extracted from Endesa company databases. Several modules were included in IES like text mining module for analyzing attributes, their relationships and extracts any additional information of the customer; a data mining module to draw up the rules of those raw data to determine the customer estimated consumption and rule based expert system module uses results of both data mining and text mining for analyzing each customer.

#### 2.4. Performance metric

Performance metric is used to determine how effective a model can be after machine learning algorithm is implemented. So for measuring the efficiency of ML algorithms, different metrics are required. The performance metrics used depend upon the datasets and the outcome of particular algorithms [21]. The main statistics used for performance metrics are regression and classification metrics. Choice of appropriate metrics can affect the whole project. For example, for prediction purpose and when an outcome is a number, root mean squared error (RMSE) is the most common metric used and for classification purposes or to distinguish between different objects, the classification performance metrics used may be log-loss, average accuracy, and AUC [22]. Generally, the performance of a classifier is evaluated by different performance indicators. One of such indicators is the confusion matrix. It denotes the details for the classification which is accurate as “True” and for the wrong classification as “False”. Costa *et al.* [10] have used confusion matrix to compare real inspections to classified inspections by the ANN-ML program which indicates four result types: i) True Positive (TP) is a fraudster consumer who is correctly classified as fraudster; ii) False Negative (FN) is a fraudster consumer who is incorrectly classified as non-fraudster; iii) False Positive (FP) is a non-fraudster consumer who is incorrectly classified as fraudster; and iv) True Negative (TN) is a non-fraudster consumer who is correctly classified as non-fraudster.

Similarly, to check for classifier efficiency some measures are checked using hit rate. Hit rate is the percentage of records correctly classified: i) Recall= $TP/(TP+FN)$ ; ii) Precision = $TP/(TP+FP)$ ; iii) TP rate= $TP/(TP+FN)$ ; iv) FP rate= $FP/(FP+TN)$ . In the NTL classification problems the metrics evaluated through the confusion matrix also include accuracy (Acc), precision, detection rate (DR). A better detection ratio and good accuracy mean the model has a good classifying ability of data in the case of both classes. However, in the scenarios where the data-sets is imbalanced there is a need for other performance metrics, i.e. if negative class samples (non-fraud) have a higher number of samples than positive type (fraudulent), in such a case DR or TP rate is used. These metrics describe the percentage of accurately classified samples of NTL to the total amount of data-sets of NTL. High DR values usually imply a well-operating NTL detection model, but other metrics also should be well considered. Therefore, both Acc and DR are to be considered when determining the efficiency of the model. Table 2 provides the list of performance metrics commonly used in evaluating NTL detection models.

Table 2. Different performance metric used

Performance metric	Calculation	References
detection rate	$DR = \frac{TP}{FN+TP}$	[1]
precision	$\frac{TP}{FP+TP}$	[10]
RMSE	Root Mean Square Error	[1]
accuracy	$accuracy = \frac{TN+TP}{TN+TP+FN+FP}$	[16]

In the scenarios of imbalanced datasets to completely evaluate the performance of the algorithm, the combination of different metrics such as precision, Acc, FP rate, TN rate and DR is utilized [16]. Whereas, Ford *et al.* [1] used RMSE measurement for determining fraudulent behavior. The data whose RMSE values are within a threshold (assigned 0.5 kW/h) were classified as normal and if not within the threshold value was considered a fraudster. In this paper neural network was used for detecting NTL. For evaluating the performance of the network the author has used a confusion matrix. The confusion matrix reports TP, TN, FP, and FN result of the network as discussed earlier [23]. The neural network was able to detect fraudulent activities in energy consumption with high level of accuracy (considered as true positive). But due to the factors like holidays, events, weather conditions, vacations, there was a frequent change in consumption behavior. These factors lead a neural network to label higher rate of normal activities as fraud, i.e. also higher FP value. Large consumption of electricity in fraudulent manner which is causing a larger demand-supply gap requires the FP to be reduced to a great extent. A scheme based on both DT and SVM for detecting the electricity thefts precisely and accurately in the complex power networks was put forward in 2016 [8]. The purposed method was able to identify fraudulent consumers with higher accuracy and also with a low FP rate. It seems DT and SVM methods work well where there are a certain number of smart meters installed. The improvement was seen in the accuracy of the SVM classifier when it was used along with DT. The scheme proves its effectiveness in real scenarios as it was used in overall power networks.

### 3. COMPARATIVE ANALYSIS AND LIMITATION OF AVAILABLE METHODS

Comparison of different aforementioned AI methods for detecting NTL is finally done based on accuracy and false positive value. The concepts of rough sets were used to reach the classification rule system. It had predicted the fraudulent consumer with a minimum rate of accuracy as compared to other methods [24]. Similarly, OPF algorithm was used to detect suspected frauds aiming to decrease the number of inspections [9]. This method particularly helped in the situation where there will be a loss of cost and time for irrelevant inspection. The use of a confusion matrix was done for measuring performance and the accuracy above average compared to the case where rough sets were used as the detection method. But, only historical data were used for performing the experiment. So the need for deeper evaluation in the field is observed. In the above mentioned articles, the fraudulent activities were introduced in a consistent manner. It was so required for building and analyzing energy consumption behavior profiles in real-time scenarios. So Ford *et al.* [1] utilized real-world historical energy consumption data for classifying the fraudulent and non-fraud activities while increasing the accuracy level. But the false positive measurement was high due to the various factors like weather, holidays, etc. causing a frequent changes in energy consumption. Unlike existing schemes, the scheme provided by Jindal *et al.* [8] was capable of precisely detecting and locating real-time electricity theft. The false positive measurement was also very low with DT fed as an input to the SVM classifier. This scheme proves its effectiveness in real scenarios which detect theft in power transmission and distribution. The used detection method of respective reviewed articles for NTL detection and correspondingly its accuracy and false positive value is analyzed in Table 3.

Table 3. Comparative analysis of AI based NTL detection methods

Detection Method	Accuracy	False Positive	Publication Year	Reference
Rough Sets	20%	Very high	2004	[24]
OPF	83.31%	Medium	2010	[9]
Fuzzy Classification	74.5%	Medium	2011	[19]
ANN-MLP	87.17%	High	2013	[10]
Expert system (GRI)	around 80%	High	2014	[12]
ANN	93.75%	High (25%)	2014	[1]
DT and SVM	92.5%	Very low (5.12%)	2016	[8]

Evidently, the supervised machine learning algorithms generally have performed eminent compared to unsupervised machine learning algorithms for detecting fraud in the energy sector. The supervised algorithm worked on labeled datasets. Therefore, somewhere when a set of references and datasets were limited it was difficult for solving the complex task by a supervised algorithm. In such a case only an unsupervised machine learning algorithm was preferred. Mostly, the supervised algorithms were used as solving methods in the area where classification and regression problems arise in energy theft. Besides selecting the method between supervised and unsupervised another important task was to select an algorithm under this method that can be best for the given problem. Every method under supervised machine learning algorithm has their own pros and cons so it was very crucial to select a suitable algorithm for a particular classification task. For example, DT is prone to overfitting mainly when the tree was particularly deep. Each data were to be re-sampled over and over and for each sample new classifier was to be trained. They are sensitive to the class imbalance and need massive time for training the models. DT required less effort for data preparation during pre-processing but if there was a small change in the structure the result was unstable and complexity have arisen in the calculation. Whereas, SVM was applied where the classes were clearly separated. It was found to be effective where the number of dimensions was greater than samples, but not suitable for large datasets. The energy consumption data required for formulating the algorithm were large in number so a huge amount of time was required for detecting the theft. It does not perform well in scenarios of overlapped classes also. Whereas in a neural network, where we can store the information on the entire network and the disappearance of a few pieces of information in one place does not prevent the network from functioning. If some household data was missing or some months data was not achieved, then also it has operated with incomplete information also. So there were no any fixed rules for determining the structure of ANN. Through experience or trial and error an appropriate network structure was achieved. Therefore, in the ANN supervised method, the duration of the network was not known for an instant.

Contrary to the supervised machine learning methods, the unsupervised machine learning method does



not require labeling data for training the model. So the unsupervised learning methods were applied where positive values, i.e, fraud consumer which was rarely present compared to that of negative values, i.e, non-fraud. It is obvious that for different types of data available, the algorithms applied perform differently. SOM an unsupervised machine learning method have many advantages for interpreting the data. The interpretation was done easily using the SOM algorithm for finding the theft in the system. The huge amount of the consumption data sets was easily tackled using the SOM which is an important factor of evaluation in energy theft detection. But the limitation of using the algorithm was that the process of training the data was slow. Also, new inputs were miss-classified after the learning process was over. But when it is once done, eventually new data can also be mapped to SOM very quickly. Whereas, Expert System in the field of AI tackles a complex problem that is difficult for human experts to evaluate. It is the method that has expert knowledge and experience in a particular field. The system provides consistent answers for repetitive decisions. But it requires to be updated manually and is not able to adapt to altering environments. Since there are no any fixed rules defined for selecting the algorithm accurately for classification of fraud and non-fraud consumers for detecting NTL in the system, the algorithms are to be selected based on the nature of the data inputs and their features which is already discussed in section 2. The review of the researches done on this topic reveals, there are many techniques based on AI technology for detecting energy fraud in the power system either in the transmission sector or at the distribution level.

#### 4. CONCLUSION AND FUTURE RECOMMENDATIONS

The paper presents a detailed review of methodologies for finding fraudulent consumer in the power distribution sector. The review focuses primarily on different ML algorithms for fraud detection in the distribution system. The different metric which is used for classifying attributes while detecting the fraud is studied. Further, based on these attributes and available datasets how ML algorithms are chosen is discussed. Different methods with their own advantage and disadvantages based on the datasets and scenarios of the consumer is studied. Since there is a lack of common data sets, classes of consumer, network topology and type of electricity theft caused, so one metric which is common on all the review papers is lacking. Only the decision is made by comparing the accuracy and FP metric of different methods. It is concluded that combing two ML algorithms to solve the theft detection problem provides better results in terms of accuracy and FP value. Also, the method is found to have worked practically in real-time scenarios to detect fraud precisely at any level of the power system. Each method has its own way of solving the problem. By combing two different techniques obviously, performance is boosted which provides better results. For getting efficient results one should make more focus on choosing suitable metric parameters along with the type of ML methods for specific problems. The methodologies of many research papers which mainly focus on the ML techniques for detecting energy fraud were studied for giving the review. It seems there is a gap in evaluating how the simulation process of fraudulent activities can be made more realistic. Actually, there is insufficient research on categorizing the NTLs detection method on one common basis. Also, there seems a need for investigating the causes of NTLs in other sectors of the power system besides the distribution sector. A deeper evaluation in the field is intended for testing different supervised classification techniques for detecting NTLs and comparing their results.

The major reason behind NTLs in the distribution system, mainly in developing countries is found to be energy theft. From different sites searched for and articles reviewed since 2009, we can analyze AI methods also have been enormously used in the field of a power system. The impact of the NTLs in the power sector is huge and should be diagnosed and prevented as soon as possible. These faults are causing a huge impact on the country's economic sector. But there seems more scarcity of research that assesses the impact of NTL in under developing countries. Contrary to that, the impact of NTL in a developed country is much less yet it is considerable. It is worthwhile to mention, there is a lack of research on assessing the financial impact of implementing the network-based methods, installation of specific sensors and smart meters. After a review, it felt there was a necessity of systematic study regarding the factors causing energy fraud in every sector of power system, i.e, both transmission and distribution system which eventually lead towards energy loss. Therefore, future studies should be done emphasizing on methods and applications where multiple solutions to a different types of fault in the power system can be done in an integrated manner considering all features or attributes causing it. Also, smart meter which enables utilities to find out the losses in the system which address about the abnormalities and sudden drop in energy consumption should be installed in a large amount. With the increment in installation of smart meters, the amount of the data generated will be more and so more precisely

any AI method can be used for improving the overall operation of the utility. Overall, NTLs need to be correctly addressed to narrow the gap between supply and demand which will eventually lead to the development of the overall power sector.





## REFERENCES

- [1] V. Ford, A. Siraj, and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," in *2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG)*. IEEE, 2014, pp. 1–6, doi: 10.1109/CIASG.2014.7011557.
- [2] J. Navani, N. Sharma, and S. Sapra, "Technical and non-technical losses in power system and its economic consequence in indian economy," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 2, pp. 757–761, 2012.
- [3] J. E. Cabral, J. O. Pinto, E. M. Martins, and A. M. Pinto, "Fraud detection in high voltage electricity consumers using data mining," in *2008 IEEE/PES Transmission and Distribution Conference and Exposition*. IEEE, 2008, pp. 1–5, doi: 10.1109/TDC.2008.4517232.
- [4] P. Glauner, C. Glaeser, N. Dahringer *et al.*, "Non-technical losses in the 21st century: Causes, economic effects, detection and perspectives," 2018.
- [5] F. Shehzad, N. Javaid, A. Almogren, A. Ahmed, S. M. Gulfam, and A. Radwan, "A robust hybrid deep learning model for detection of non-technical losses to secure smart grids," *IEEE Access*, vol. 9, pp. 128 663–128 678, 2021, doi: 10.1109/ACCESS.2021.3113592.
- [6] I. Vlasa, A. Gligor, C.-D. Dumitru, and L. B. Iantovics, "Smart metering systems optimization for non-technical losses reduction and consumption recording operation improvement in electricity sector," *Sensors*, vol. 20, no. 10, p. 2947, 2020, doi: 10.3390/s20102947.
- [7] M. S. Saeed, M. W. Mustafa, N. N. Hamadneh, N. A. Alshammari, U. U. Sheikh, T. A. Jumani, S. B. A. Khalid, and I. Khan, "Detection of non-technical losses in power utilities—a comprehensive systematic review," *Energies*, vol. 13, no. 18, p. 4727, 2020, doi: 10.3390/en13184727.
- [8] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and svm-based data analytics for theft detection in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1005–1016, 2016, doi: 10.1109/TII.2016.2543145.
- [9] C. C. O. Ramos, A. N. de Sousa, J. P. Papa, and A. X. Falcao, "A new approach for nontechnical losses detection based on optimum-path forest," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 181–189, 2010, doi: 10.1109/TPWRS.2010.2051823.
- [10] B. C. Costa, B. L. Alberto, A. M. Portela, W. Maduro, and E. O. Eler, "Fraud detection in electric power distribution networks using an ann-based knowledge-discovery process," *International Journal of Artificial Intelligence & Applications*, vol. 4, no. 6, p. 17, 2013, doi: 10.5121/ijaia.2013.4602.
- [11] V. Sessions and M. Valtorta, "The effects of data quality on machine learning algorithms," *ICIQ*, vol. 6, pp. 485–498, 2006.
- [12] C. León, F. Biscarri, I. Monedero, J. I. Guerrero, J. Biscarri, and R. Millán, "Variability and trend-based generalized rule induction model to ntl detection in power companies," *IEEE Transactions on Power Systems*, vol. 26, no. 4, pp. 1798–1807, 2011, doi: 10.1109/TPWRS.2011.2121350.
- [13] C. Leon, F. Biscarri, I. Monedero, J. I. Guerrero, J. Biscarri, and R. Millán, "Integrated expert system applied to the analysis of non-technical losses in power utilities," *Expert systems with applications*, vol. 38, no. 8, pp. 10 274–10 285, 2011, doi: 10.1016/j.eswa.2011.02.062.
- [14] J. V. Spirić, S. S. Stanković, M. B. Dočić, and T. D. Popović, "Using the rough set theory to detect fraud committed by electricity customers," *International Journal of Electrical Power & Energy Systems*, vol. 62, pp. 727–734, 2014, doi: 10.1016/j.ijepes.2014.05.004.
- [15] B. Coma-Puig, J. Carmona, R. Gavalda, S. Alcoverro, and V. Martin, "Fraud detection in energy consumption: A supervised approach," in *2016 IEEE international conference on data science and advanced analytics (DSAA)*. IEEE, 2016, pp. 120–129, doi: 10.1109/DSAA.2016.19.
- [16] X. Lu, Y. Zhou, Z. Wang, Y. Yi, L. Feng, and F. Wang, "Knowledge embedded semi-supervised deep learning for detecting non-technical losses in the smart grid," *Energies*, vol. 12, no. 18, p. 3452, 2019, doi: 10.3390/en12183452.
- [17] M. Sodenkamp, K. Hopf, and T. Staake, "Using supervised machine learning to explore energy consumption data in private sector housing," in *Handbook of research on organizational transformations through big data analytics*. IGI Global, 2015, pp. 320–333, doi: 10.4018/978-1-4666-7272-7.ch019.
- [18] L. A. P. Júnior, C. C. O. Ramos, D. Rodrigues, D. R. Pereira, A. N. de Souza, K. A. P. da Costa, and J. P. Papa, "Unsupervised non-technical losses identification through optimum-path forest," *Electric Power Systems Research*, vol. 140, pp. 413–423, 2016, doi: 10.1016/j.epr.2016.05.036.
- [19] E. W. S. Angelos, O. R. Saavedra, O. A. C. Cortés, and A. N. de Souza, "Detection and identification of abnormalities in customer consumptions in power distribution systems," *IEEE Transactions on Power Delivery*, vol. 26, no. 4, pp.





- 2436–2442, 2011, doi: 10.1109/TPWRD.2011.2161621.
- [20] C. Boucetta, O. Flauzac, A.-N. M. Nassour, and F. Nolot, “Multi-level hierarchical clustering algorithm for energy-theft detection in smart grid networks,” in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2020, pp. 1–6, doi: 10.1109/ICECCE49384.2020.9179334.
- [21] M. Sunasra, “Performance metrics for classification problems in machine learning,” *Medium recuperado de: <https://medium.com/thalusai/performance-metrics-for-classification-problems-in-machine-learningpart-i-b085d432082b>*, 2017.
- [22] C. Ferri, J. Hernández-Orallo, and R. Modroiu, “An experimental comparison of performance measures for classification,” *Pattern Recognition Letters*, vol. 30, no. 1, pp. 27–38, 2009.
- [23] S. Visa, B. Ramsay, A. L. Ralescu, and E. Van Der Knaap, “Confusion matrix-based feature selection,” *MAICS*, vol. 710, pp. 120–127, 2011.
- [24] J. E. Cabral and E. M. Gontijo, “Fraud detection in electrical energy consumers using rough sets,” in *2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583)*, vol. 4. IEEE, 2004, pp. 3625–3629, doi: 10.1109/ICSMC.2004.1400905.

## BIOGRAPHIES OF AUTHORS



**Sushmita Poudel**     is an Electrical engineer. She received Bachelor’s Degree in Electrical and Electronics Engineering from Pokhara University, School of Engineering, Lekhnath 30, Pokhara, Nepal in 2017. At present she is student of Master of Science in Electrical Engineering in Power System in same institution. Her research interests include Smart Grid, Renewable Energy, Power System, Distribution Management System (DSM), Artificial Intelligence and the areas of optimization and control. She can be contacted at email: sushmitapoudel18@gmail.com.



**Dr. Udaya Raj Dhungana**     grew in a beautiful city Pokhara, Nepal, is the inventor of PolyWordNet- a lexical database that organizes the senses of polysemy words based on their related words. He achieved Doctor of Philosophy (PhD) in Computer Engineering from Institute of Engineering, Tribhuvan University, Nepal under the Young PhD Fellowship granted by University Grant Commission, Nepal. He also received Erasmus Mundus Action 2 Scholarship under IDEAS project for his PhD research at Darmstadt University of Applied Sciences, Germany from Sept, 2014 to Jun, 2015. During his research stay at Darmstadt, one of his research papers is awarded as the best research paper in IEEE conference CICSyN 2015, Riga, Latvia. He obtained Master of Engineering (ME) in Computer Engineering from Kathmandu University, Nepal in 2011 and Bachelor of Computer Engineering from Pokhara University, Nepal in 2005. He is an Assistant Professor at School of Engineering, Pokhara University since 2013. He served as an ICT Director at Pokhara University from 2017 to 2019. He is also working at the Darmstadt University of Applied Sciences as a Guest Faculty since 2018. In addition, he is the coordinator of Erasmus+ scholarship project between Darmstadt University of Applied Sciences and Pokhara University since 2019. His research interest includes the Word Sense Disambiguation, Lexical Database, Knowledge Representation, Expert System and Automatic Question Answering. He can be contacted at email: udaya@pu.edu.np.