Energy Reports 12 (2024) 3048–3064

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Machine-learning techniques for enhancing electricity theft detection considering transformer reliability and supply interruptions

Yu-Chung Tsao [a,b,*], Dinita Rahmalia [a], Jye-Chyi Lu [c]

[a] Department of Industrial Management, National Taiwan University of Science and Technology, Taipei, Taiwan
[b] Artificial Intelligence for Operations Management Research Center, National Taiwan University of Science and Technology, Taipei, Taiwan
[c] School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, USA

ARTICLE INFO

Keywords:
Fraud detection
Data mining
Interruption
Reliability
Smart grid

ABSTRACT

Machine-learning techniques are extensively used in fraud detection and have a huge potential application in electricity theft detection. Electricity theft occurs when consumers manipulate their electricity consumption to be recorded as lower than the actual, resulting in reduced revenue for the electricity supplier. This study explores the application of advanced machine-learning techniques to detect electricity theft, focusing on the impact on supply of electricity to electricity usage pattern. We used a dataset that contains supply interruptions influenced by transformer reliability to construct a robust detection model. This model integrates data analytic techniques from decision trees, support vector machines, k-nearest neighbors, and logistic regression classifiers. After selecting the optimal classifier, we used aggregated parameters to improve theft-detection accuracy. A comprehensive sensitivity analysis was used to evaluate the effects of variations in transformer reliability factors on interruption, interruption costs, electricity revenue, and theft-detection performance. Our findings indicate that using optimal aggregated parameters significantly enhances detection accuracy 10.709 percent, 11.435 percent, 4.909 percent, and 2.097 percent from original parameters depend on the number of aggregation in 2-hour, 4-hour, 6-hour, and 12-hour, respectively. The lower transformer reliability leads to increased loss with percentage 66.87 percent, 46.98 percent, 17.22 percent and reduced theft-detection efficiency by 27.32 percent, 19.23 percent, 6.20 percent. depend on reliability factor20 percent, 50 percent, and 80 percent, respectively.

1. Introduction

In the smart-grid environment, electricity is distributed from power plants to end users or customers via transmitting stations. Two-way communication networks exist between transmission and distribution substations (Judge et al., 2022). By using advanced technologies, smart grids can deliver power and electricity in a well-organized manner. One of the latest technologies for smart-grid environments is the smart meter installed at customer sites. A smart meter is an electronic device that records information such as electricity consumption, voltage level, and current load. However, smart meters can be manipulated by some customers to record lower than actual power consumption, resulting in lower electricity revenue for the supplier.

The design of a real-time electricity theft detection in distribution systems had been developed by Zulu and Dzobo, (2023). This proposed system used smart meters consisting of an Arduino ATMega328P microcontrollers with GSM modules (Global System for Mobile Communication) for system communication. Then the smart meter data were stored on the cloud storage. The power from transmission flow to area network. The smart meters are installed in the area network and show electricity consumption. The information are delivered two ways to system operators.

Theft detection is crucial as it safeguards the revenue of electricity suppliers. In 2015, India experiences widespread cases of electricity theft, with 16.6 billion dollars lost to electricity theft (Lepolesa, et al., 2022). Also, in Brazil and Russia, power companies lost approximately 10.5 and 5.1, billion dollars in year of 2015, respectively. In 2019, South Africa suffered 1.31. billion dollars (Louw, Bokoro, 2019). Theft detection is a kind of fraud detection, that is, a process for identifying and preventing fraudulent activities. It can be achieved by monitoring and investigating customer behavior patterns for anomalies. Some studies have focused on the implementation of credit card fraud detection (Cherif, et al., 2023; Nalayini, et al., 2023; Carcillo, et al., 2021; Izotova, Valiullin, 2021; Lei, et al., 2023; Bahnsen, et al., 2016; Roseline, et al., 2022), in finance, accounting, and insurance (Sadgali, et al., 2019;

* Corresponding author at: Department of Industrial Management, National Taiwan University of Science and Technology, Taipei, Taiwan.
E-mail address: yctsao@mail.ntust.edu.tw (Y.-C. Tsao).

https://doi.org/10.1016/j.egyr.2024.08.068
Received 15 June 2024; Received in revised form 12 August 2024; Accepted 24 August 2024
Available online 8 September 2024

Nomenclature

ANN	Artificial Neural Network
CAIDI	Customer Average Interruption Duration Index
CNN	Convolutional Neural Network
DT	Decision Tree
FN	False Negative
FP	False Positive
GSM	Global System for Mobile Communication
KNN	K-Nearest Neighbour
LR	Logistic Regression
NB	Naive Bayes
RF	Random Forest
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Duration Index
SVM	Support Vector Machine
TN	True Negative
TP	True Positive
c_{jk}	The selection of classifier j at block k
C_k^{FN}	The set of customers at block k involved in False Negative cluster
C_k^{FP}	The set of customers at block k involved in False Positive cluster
C_k^{TN}	The set of customers at block k involved in True Negative cluster
C_k^{TP}	The set of customers at block k involved in True Positive cluster
f_{itk}	Normal electricity usages of customer i at block k on time t
g_{itk}	Fraudelent electricity usages of customer i at block k on time t
I^R	Interruption cost in pounds per hour for residential customers
I^C	Interruption cost in pounds per hour for commercial customers
I^A	Interruption cost in pounds per hour for agricultural customers
I^I	Interruption cost in pounds per hour for industrial customers
I^P	Interruption cost in pounds per hour for public customers
N_{block}	The number of blocks
N_{cust}	The number of customers
O_{ijk}	The output of classifier j of customer i at block k
d_{ik}	Fines on customer i at block k
n_{ik}	Customer i at block k experiencing interruption
p_{ik}	Electricity price per kWh for on customer i at block k
q_{ik}	Repairing cost for the detector that misclassify on customer i at block k
r_{ik}	Interruption duration on customer i at block k
U_R	The set of residential customers
U_C	The set of commercial customers
U_A	The set of agricultural customers
U_I	The set of industrial customers
U_P	The set of public customers
v_{ijk}^{FN}	The selection of classifier j on customer i at block k involved in False Negative cluster
v_{ijk}^{FP}	The selection of classifier j on customer i at block k involved in False Positive cluster
v_{ijk}^{TN}	The selection of classifier j on customer i at block k involved in True Negative cluster
v_{ijk}^{TP}	The selection of classifier j on customer i at block k involved in True Positive cluster
y_{ik}	The target of customer i at block k
Z^{FN}	Penalty terms due to misclassifying False Negative
Z^{FP}	Penalty terms due to misclassifying False Positive

Aslam, et al., 2022; Mao, et al., 2021; Mohan, Praveen, 2019). Credit card fraud detection works by considering transaction ID, time, account number, card number features, and decision for transaction success or failure.

Class imbalance is often encountered when dealing with fraud detection as research done by Lepolesa et al., (2022), Yang et al., (2023). Class imbalance occurs when the proportions of samples with normal and abnormal conditions have a large disparity. Solutions to these problems include oversampling, undersampling, and hybrid sampling. To perform the better results, Bagga et al., (2020) developed ensemble methods referring to the combination of various estimator built by a specific learning method for improving individual a single estimator. Reddy et al., (2024) used stack generalization of seven classifiers i.e. Logistic Regression (LR), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), Naive Bayes (NB), and Gradient Boosting (GB). In a stacking model, each model made a forecast, and then there was a meta-model that took all predictions and used them to make a final prediction.In this study, we detected fraud through electricity theft detection. Unlike many fraud detection studies that focus on different independent explanatory features, in electricity theft detections, time-series data such as hourly electricity usage are used as inputs. Furthermore, Haq et al. had developed time series data into Convolutional Neural Network (CNN) model for electricity theft detection and reducing low accuracy caused by unbalanced dataset. We applied “theft-case generators” based on electricity usage to avoid class imbalances. Machine-learning techniques are quite popular in solving theft detections; in this study, we employed a combination of DT, SVM, KNN, NB, and LR to analyze electricity usage data.

One of methods to improve the accuracy is aggregating the parameters. Since time series data are continuous and identical, the data can be aggregated to be shorter, which can affect the accuracy of electricity theft detection. Electricity theft detection using time series feature data as in Lepolesa, et al., (2022), Haq, et al., (2023), Stracqualursi, et al., (2023), Li, et al., (2019), Wang, et al., (2023), Liao, et al., (2024), Khan, et al., (2020), Zidi, et al., (2023), and Jokar, et al., (2016) did not show the effect of aggregating time series data to detection accuracy. This research compares the accuracy between original time series data and aggregated time series data. According to Zidi, et al. (2023), electricity theft detections were worked only by employing the pattern consumption of electricity and their theft manipulations divided by six theft types. Since the electricity usages are affected by interruption of electricity, the theft manipulation patterns are also changed. This research considers the accuracy of electricity theft detection and its influences

This study aims to answer the following research questions:

- How the effects of aggregated parameters into accuracies of electricity theft detection?
- What methods are proposed to classify the electricity theft?
- How the effects of transformer reliability and interruptions into accuracies of electricity theft detection?

The main contributions of this study are as follows:

- Customer electricity consumption in residential, commercial, industrial, agricultural, and public sectors was monitored and investigated. Substantial anomalies in electricity consumption indicate

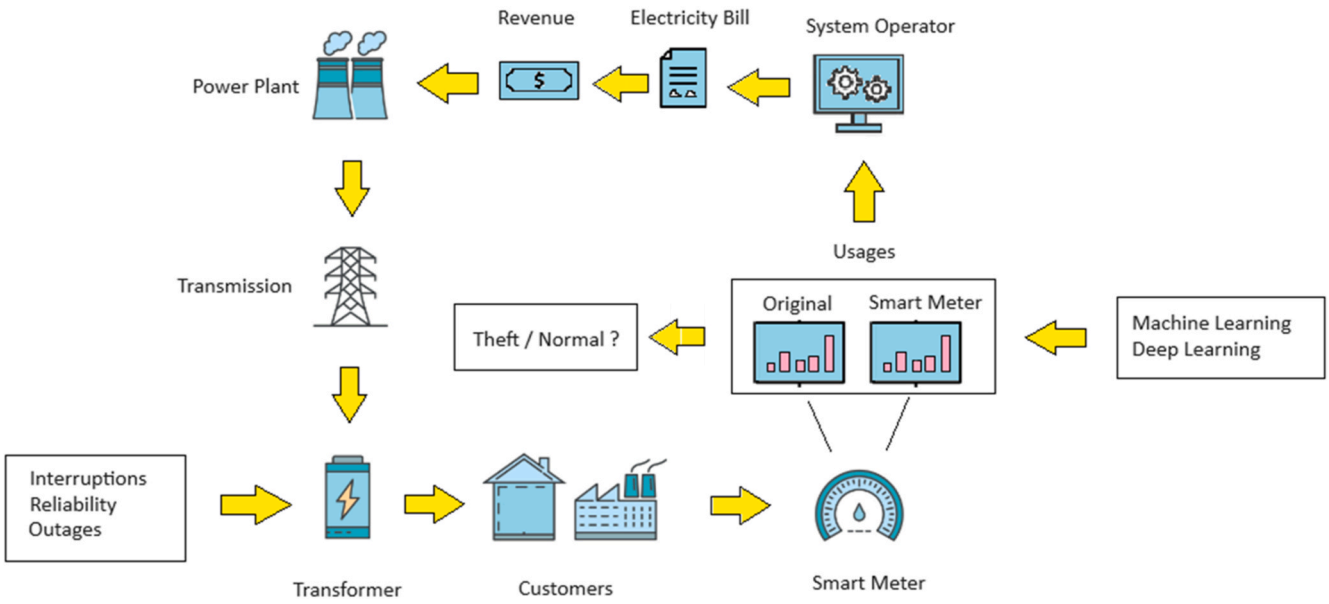

Fig. 1. The overview of work.

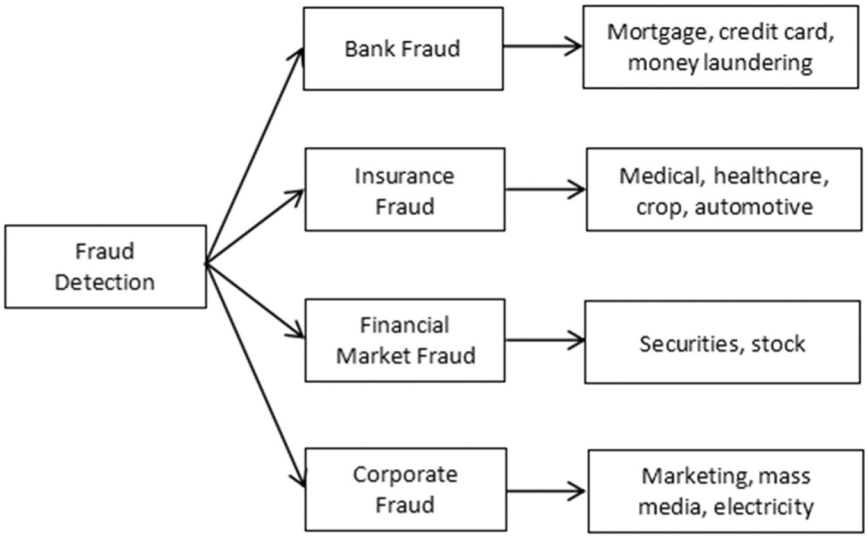

Fig. 2. Fraud detections in many sectors.

potential electricity theft. The study highlights the advantages and disadvantages of installing smart meters in every home.

- From a theoretical perspective, this study suggests ways to improve classification accuracy and aggregate parameter inputs. When the parameter inputs or features of the training data are not too small or too long, the proposed method achieves good accuracy with minimum misclassification.
- The reliability factor of the transformer distributing electricity to homes affects interruption costs. Because interruption interferes with the production of customers, leading to loss, this study exposes the impact of the reliability factor on customers and the need for power suppliers to maintain their transformers regularly. Power interruption also impacts electricity revenue and theft-detection performance.

The remainder of this paper is organized as follows. The review of literature related to fraud detection, electricity theft detection, and power interruption is presented in Section 2. Machine-learning classifiers are discussed in Section 3. Section 4 presents the construction of the mathematical model for electricity theft detection. Numerical results and sensitivity analyses are explained in Section 5. Section 6 concludes the paper. Fig. 1

2. Literature review

The model of electricity theft detections almost resemble to fraud detection, such comparing the two different conditions, and giving the binary label to the output. In the fraud detection, there are two conditions, original condition and practical condition, with each condition has some parameters to be investigated. When there are any parameters that show anomalies between original and practical condition, then they affect to label the output. Khodabandehlou and Golpayegani, (2022) divided fraud detection in many sectors such as bank, insurance, financial market, and corporate as in Fig. 2. In the electricity theft detection, the time series data of electricity usage are used as parameters. When there are differences between usage in original condition and

Fig. 3. Information flow of electricity theft.

practical condition, then the possibility of electricity theft will be formed.

2.1. Machine learning on fraud detection

Machine learning has been applied to fraud detection in many areas, especially in finance. Cherif et al. (2023) reviewed how to detect fraud using either traditional machine learning or deep learning and also how to handle mchine-learning problems like class imbalance. For the class imbalance, they suggested oversampling, under sampling, and hybrid sampling. Sadgali et al. (2019) showcased machine-learning performance in financial-fraud detection by classification, clustering, and regression. Hilal et al. (2022) investigated anomaly detection in financial fraud using semi-supervised and unsupervised learning. Supervised anomaly-detection techniques use labeled datasets that show the normal and anomalous classes. Semi-supervised anomaly-detection techniques use datasets with labels for the data belonging to the normal class only, whereas unsupervised anomaly-detection techniques require no class labels. Nalayini et al. (2023) identified credit card fraud using a CNN with a smart matrix algorithm. Blaszczynski et al. (2021) used a dominance-based rough set approach to handle the problem of class imbalance while detecting auto loan fraud and the method outperformed RF and SVM. In their model, they removed some attributes, such as marital status, gender, number of children, number of people in households, legal form used, net asset, annual turnover, annual cost, annual income for the prior year, number of employees, and company age. Carcillo et al. (2021) combined unsupervised and supervised learning on credit card fraud detection and the combination was efficient; it improved detection accuracy. Izotova, Valiullin, (2021) compared the Poisson process with a machine-learning algorithm in determining the probability of fraud prediction. Aslam et al. (2022) found fault, base policy, and age of policyholder as the most influential features in insurance fraud detection using LR, SVM, and NB. Lei et al. (2023) proposed a deep neural network model to curb privacy leakage and reduce data-handling costs in credit card fraud detection. Mao et al. (2021) proposed a related party transaction knowledge graph to mine valuable hidden knowledge from large-scale associated data as a new form of knowledge representation. Mohan, Praveen, (2019) detected fraud in medical insurance claims committed by using wrong details, modifying identities, fake documentation, and double billing. Sadiq et al. (2019) applied SVM based on multiverse feature extraction for smart city applications. Chouiekh and Haj, (2018) suggested a deep CNN (DCNN) rather than SVM, random forest, and gradient boosting to analyze fraud detection. Bahnsen et al. (2016) used a transaction-aggregation strategy to predict fraud based on transaction ID, time, account number, card number, transaction type, entry mode, amount, merchant code, country, type of card, and bank. Roseline et al. (2022) constructed a long short-term memory-recurrent neural network to predict autonomous credit card fraud detection. Jessica et al. (2023) used LR, RF, KNN, and XGBoost in credit card fraud detection based on transaction time. Aschi et al. (2022) suggested batch layer and stream layer in the model training and the real time fraud detection is based on new input transaction data. Bagga et al. (2020) optimized credit card fraud detection using pipelining and ensemble learning. Reddy et al. (2024) applied individual classifiers and stack generalization consisting of bagging and boosting. Chen et al. (2020) suggested hybrid scoring model on fraud detection. The LR algorithm is joined with weighted evidence to fabricate another score model. Liu et al. (2024) utilized ensemble learning and stacking generalization techniques that combined predictions.

The fraud detections were not only encountered in simple features such as ID, transaction time, amount of money, etc. In advances, some image features could be manipulated to be fraudulent. Lin et al. (2023) used CNN to detect heterologous and homogenous manipulations. Bai (2024) proposed multi-scale contrasive learning for image manipulation detection and localization. The Adaptive Self Attention Module (ASAM) was utilized to filter and aggregate the relevant context. Thakur and Rohilla, (2020) classified manipulation detection techniques such as copy-move and splicing manipulations, universal image manipulations, compression image manipulations, and miscellaneous manipulations. Yadav and Vishwakarma, (2023) proposed architecture that extracted discriminative manipulation residuals and textural features for facial manipulation detections. Xiao et al. (2023) used deep forgery detection method for key populations under information measurement. Samanta and Jain, (2021) analyzed perceptual hashing algorithms in image manipulation detection. Camacho and Wang, (2022) focused on the variance stability for the output of convolutional filter in CNN for image manipulation detection.

2.2. Electricity theft detection

The power flow from transmission, customers with smart meters, until system operators can be seen in Fig. 3. When the electricity is received by customers, smart meter will measure the power usage per hour. The results are delivered to system operator for computing the electricity bill. Customers have possibilities to manipulate their electricity usage on smart meters. These behaviors can be pointed as electricity theft. Stracqualursi et al. (2023) reviewed the benefits and limitations of artificial intelligence to specific thefts. Zulu and Dzobo, (2023) used smart meters consisting of an Arduino ATMega328P microcontroller. When power imbalances were measured by the system, the authority office would receive a power-theft notification detected by the smart meter system. Lepolesa et al. (2022) addressed the missing class and class imbalance problems through data interpolation and synthetic-data generation. Haq et al. (2023) used DCNN when machine learning had drawbacks in processing unstable data.

Yang et al. (2023) developed a multi-view broad learning system for electricity theft detection since the model suffered underfitting owing to high dimensionality and imbalanced class distribution. Lie at al. (2019) detected electricity theft by incorporating CNN and random forest. They also considered electricity consumption during working days, holidays, and by seasons. Zhao et al. (2024) proposed a combination of detection models that extracted local and global features of data. They added gamma noise to a user power consumption data to preserve user privacy without adversely affecting detection accuracy. Wang et al. (2023) considered a decentralized federating-learning framework to train the model and compared it with a centralized model. Liao et al. (2024) constructed a graph attention network to improve detection accuracy from a fresh viewpoint on a graph domain. Khan et al. (2020) implemented an extreme gradient boosting based on a firefly algorithm. Furthermore, state-of-the-art methods were also implemented for comparison, that is, SVM, CNN, and LR. Zidi et al. (2023) modeled an

Table 1
Review of collected articles.

No	Ref.	Electricity Theft Detection	Electricity Interruption	The Interruption Effectsto Electricity Theft Detection
1	Zulu, Dzobo, (2023)	v		
2	Lepolesa, (2022)	v		
3	Haq (2023)	v		
4	Yang (2023)	v		
5	Li (2019)	v		
6	Zhao (2024)	v		
7	Wang (2023)	v		
8	Liao (2024)	v		
9	Khan (2020)	v		
10	Fogliatto (2022)		v	
11	Usberti (2023)		v	
12	Antaneh (2021)		v	
13	Vidovic (2021)		v	
14	Forcan, Forcan, (2022)		v	
15	Achariyakul, Rerkpreedapong, (2022)		v	
16	This paper	v	v	v

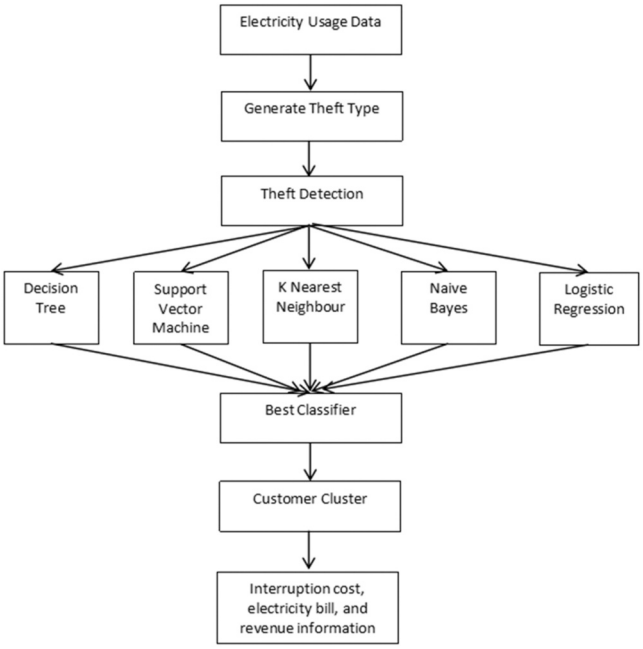

Fig. 4. Flowchart of theft detection.

effective theft generator and used KNN, DT, RF, bagging ensemble, and ANN for classification. Jokar et al. (2016) used customer consumption patterns based on theft detectors to identify theft.

2.3. Power distribution system interruption

Power interruptions are caused by component outages so that the power can not flow regularly. Fogliatto et al. (2022) found lognormal as the best distribution for interruption duration time models, and they used regression analysis for estimation. Usberti et al. (2023) created a flow-based framework for the reliability assessment of energy networks. Antaneh et al. (2021) showed that the optimal placement of tie switches could reduce power losses, total cost of outages, and reliability indices. Vidovic et al. (2021) proposed a new power flow model and calculation procedure for distribution networks with simultaneous phase interruption. Forcan and Forcan, (2022) used mixed integer linear programming and long-term load forecasting for optimal placement of remote-controlled switches. Achariyakul and Rerkpreedapong, (2022) determined a feeder failure rate to evaluate the likelihood of future interruptions.

In this study, we offered the new idea in integration of machine learning applications affected to reliability factor of transformer that cause electricity interruptions. The interruption of electricity depends on the reliability of transformers. When interruptions take place, the revenue of power plant will be decreasing and the customer in many sectors area can not be productive causing the loss production and interruption cost. When there are several customer cheating by manipulating the power usage, they will be complicated to be identified as long as no power supply in any interval time.We collected references about machine learning for electricity theft detection and interruption studies, as in Table 1.

3. Machine learning classifiers

The dominant methods for theft detection are using machine-learning classification. In machine-learning classification, the dataset is split into training data for obtaining the optimal model parameters and testing data for testing the model. The optimal classification performance is maximizing the accuracy between the target and output. Other classification-performance metrics using accuracy and error rate are calculated as in Equation (1) and Eq. (2) respectively:

$$\text{Accuracy}: \frac{\boldsymbol{TP}+\boldsymbol{TN}}{\boldsymbol{P}+\boldsymbol{N}} \times \mathbf{100\%} \tag{1}$$

$$\text{Error rate}: \frac{\boldsymbol{FP}+\boldsymbol{FN}}{\boldsymbol{P}+\boldsymbol{N}} \times \mathbf{100\%} \tag{2}$$

With:

N (Negative) is the number of normal usage

P (Positive) is the number of fraudulent usage

TN(True Negative) is the normal usage counts that are correctly labeled as normal usage

TP (True Positive) is the fraud usage counts that are correctly labeled as fraud usage

FN(False Negative) is the fraud usage counts that are incorrectly labeled as normal usage

FP (False Positive) is the normal usage counts that are incorrectly labeled as fraud usage

The flowchart in Fig. 4 shows how theft-detection algorithms work. From the electricity usage dataset for 24 h, we created a time-series dataset consisting of fraud electricity usage as a representation of theftusing theft generator algorithm. The normal usage time series were compared with fraud usage time series. When the fraud equals with original, then the output is normal usage. In other hand, when fraud is different with original, then there is indication as theft. Then, we compared five classification models: DT, SVM,KNN, NB, and LR and experimented with aggregated parameters. The five method classifiers work, started from handling missing values in preprocessing data, training data, and testing data. The dataset consist of 30 blocks and each block has 50 customers. Each block has best classifier that will be used as decision. When the classifier decision has been obtained, the accuracy can be computed and information about customer cluster (TN, TP, FN, FP) are used for computing electricity revenue. The electricity revenue is calculated by fraud usage time series. When the fraud usage is lower than normal usage, the electricity revenue will be lower rather than normal usage. In the objective, we give penalty if any misclassifications take place. We added interruption data based on reliability to the electricity usage and observed how interruption data affect classification performance. From the classification results, we can compute interruption costs and power plant revenue loss.

Five different classifiers have different control parameters. The electricity theft detection uses time series as continuous variables for

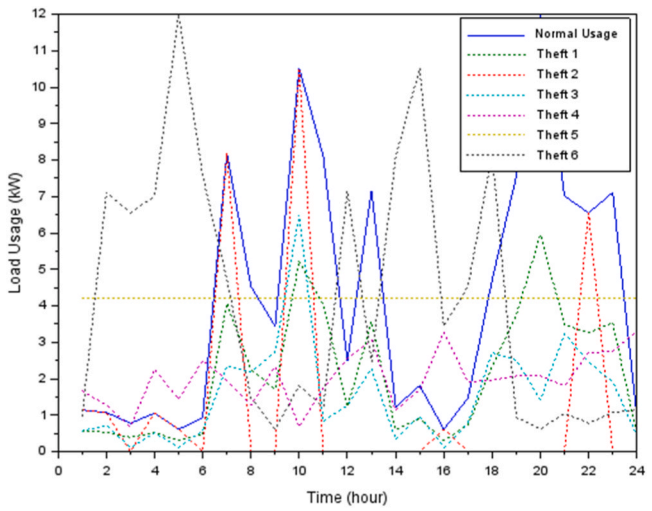

Fig. 5. Comparison graph in normal usage and fraud usage.

classification. For DT and NB, where they utilize categorical variable, then continuous variables should be categorical by a certain number. Many numbers are tried for categorizing the continuous variables until maximum accuracy avoiding underfitting and overfitting in training data. DT uses entropy and information gain for making branch and determining classification at the leaves, while NB uses conditional probability and Bayes theorem. For SVM, the optimal margin equation is used for separating the class with maximum accuracy. The optimal margin equation are obtained from optimal lagrange multiplier parameters computed by quadratic programming. For KNN, we apply K=5 of the nearest distances. For LR, the optimal logistic function is used for determining probability as theft, since the theft is notated by 1, with maximum accuracy. The optimal parameters of logistic function are obtained from first derivative of loss function.

The stopping criteria for training data is reaching accuracy between 50 % and 90 %. When the training data accuracy falls under 50 %, it occurs underfitting, and when the training data accuracy falls above 90 %, it occurs overfitting. Both underfitting and overfitting in training data will give low accuracy in testing data.

For validation the results, we use K Fold Cross Validation by dividing the dataset to be K partitions. For each partition, the accuracy is calculated. After the accuracies of all partitions have been measured, we compute the accuracy mean of all partitions. Based on validation, the accuracy of validation data is the neighbourhood training data accuracy and testing data accuracy.

The objective of this study was to determine the classifier that best identifies electricity theft. We classified theft into Types 1, 2, 3, 4, 5, and

Table 2
Comparison results from previous research.

Research	Classifiers	Original		Undersampling		Research	Classifiers	Number of instances	Accuracy
		Number of instances	Accuracy	Number of instances	Accuracy				
Zidi, et al., (2023)	KNN	560640	84.91	50	73.33	This paper	DT	50	66.67
	DT	560640	82.67	50	70.00		SVM	50	69.10
	RF	560640	85.00	50	76.67		KNN	50	71.77
	Bagging	560640	84.85	50	66.67		NB	50	60.47
	ANN	560640	80.49	50	73.33		LR	50	72.20
Jokar, et al., (2016)	SVM	535	76.00	50	63.33				

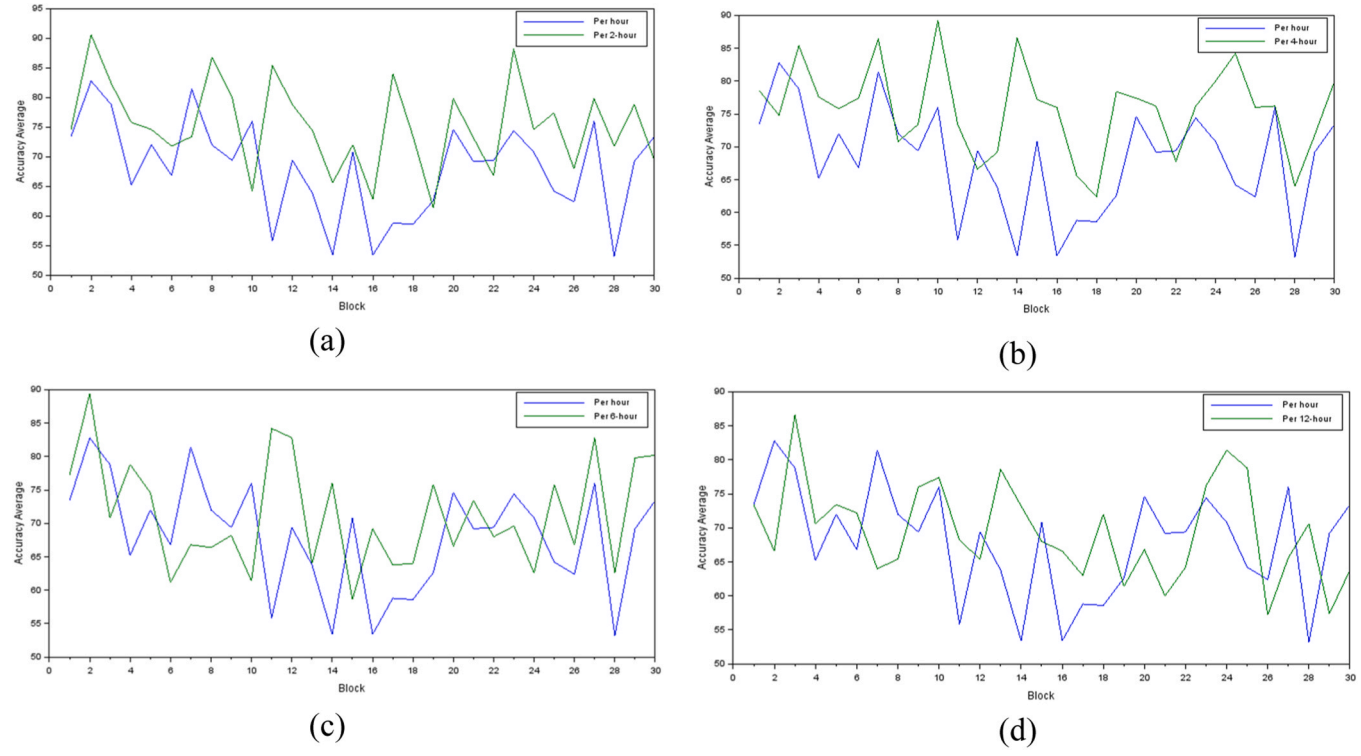

Fig. 6. The comparison of average accuracies on original dataset with aggregated dataset (a) Using per two-hour data (b) Using per four-hour data (c) Using per six-hour data (d) Using per twelve-hour data.

Table 3
Accuracy of Five Classifier Methods and Improvement Percentage.

Classifier Method	Experiment 1	Experiment 2	Experiment 3	Experiment 4	Experiment 5
DT	66.67	75.83	73.73	73.80	70.73
SVM	69.10	75.30	77.80	74.17	72.77
KNN	71.77	80.40	82.83	76.47	76.93
NB	60.47	68.97	66.70	59.57	57.73
LR	72.20	76.13	78.03	72.90	69.17
Average	68.042	75.326	75.818	71.380	69.466
Percent Improvement	-	10.709	11.435	4.909	2.097

Table 4
Statistical analysis of aggregating parameters.

Experiment pair	P-Value	Conclusion
Experiment 1 & Experiment 2	0.000	Significant. Accuracy by aggregating 2-hour is increasing
Experiment 1 & Experiment 3	0.000	Significant. Accuracy by aggregating 4-hour is increasing
Experiment 1 & Experiment 4	0.046	Quite significant. Accuracy by aggregating 6-hour is quite increasing
Experiment 1 & Experiment 5	0.226	Not significant. Accuracy by aggregating 12-hour is not increasing

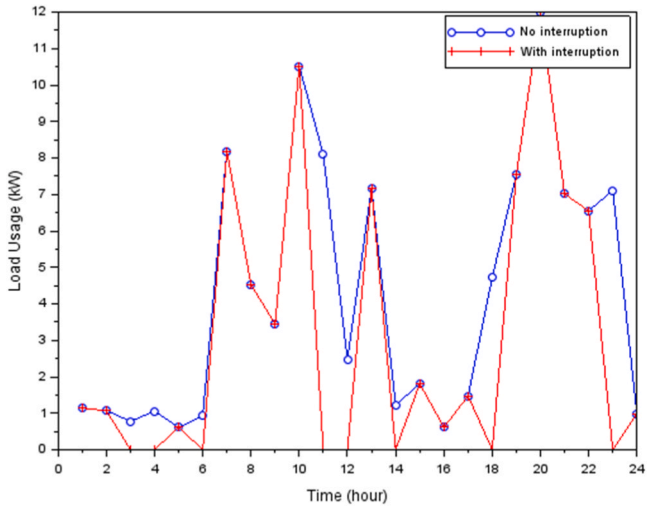

Fig. 7. Electricity usage without and with interruption.

6. All theft types are notated by 1 for theft and 0 for normal usage. We used the performance metrics of accuracy (the more the TN and TP numbers the better the classifier). When the classifier misclassifies (FN or FP), then there are repairing costs imposed on the objective function. We then subtract the repairing cost from the electricity revenue, which reduces electricity revenue.

Several classifiers are used for electricity theft detection; these are often compared and the best one is chosen. We used customer cluster information (TN, TP, FN, FP) from the best classifier to compute 24-hour electricity revenue. The objective function of the model had a linear combination form that is a modification of accuracy formula. Since the accuracy formula equals the ratio of TP and TN with entire sets of P and N, the objective function was modified to reflect the amount of electricity revenue both under normal and fraud situations, detected or not, and when misclassifications occurred, we subtracted repairing cost and multiplied with penalty term. When fraud was predicted, we allocated the unpaid cost so that the revenue reflected normal usage. When TP was detected, we added the fines which contribute to the electricity revenue.

Interruption cost is the cost of production loss to the customer when electricity supply fails. In other words, customers lose their productivity because there is no electricity supply. Interruption costs are various depend on customer type (residential, agricultural, industrial, commercial, and public). More interruptions are indicated by the value 0 kW during the time interval of electricity usage, reducing the electricity revenue. In profit calculation, there are two objectives, that is. electricity revenue and interruption cost. In the multi-objective technique, we implemented the weight technique to compute the single objective.

Penalty cost in the objective function is the repairing cost when misclassifications occur. In practice, the company incurs costs when repairing malfunctioning smart meters. Moreover, we add the fines imposed on the TP group, which increase revenue. The penalty cost is the same for all theft types because we assume theft Types 1,2,3,4,5, and 6 as general theft.

Table 5
Interruption cost according to customer type (Pounds/kWh).

Customer Type	Interruption Cost (Pounds/kWh)
Residential	0.32
Commercial	0.44
Industrial	0.496
Agricultural	0.48
Public	0.456

4. The theft detection mathematical model

We constructed an optimization model of theft detection that combines machine-learning accuracy optimization. The classification output of machine learning was used to compute electricity revenue for each customer cluster(TN, TP, FN, FP). After that, we added the interruption data to the objective function.

4.1. Theft detection

To simulate theft detection from the hourly electricity usage dataset, we applied an algorithm to generate theft types. The advantage of generating theft types is avoiding class imbalances because we can determine the proportion of normal and fraud usage. When the code is fraud, we generate six types of theft:

Suppose that $X = \{x_1, x_2, ..., x_{24}\}$ where represents electricity consumption at time (hour) x. The algorithm for generating six theft types are

$$Theft1(x_i) = \alpha x_i \quad \alpha \sim U(0.1, 0.8), i = 1, 2, \ldots, 24$$

$$Theft2(x_i) = \beta_i x_i \quad i = 1, 2, \ldots, 24$$

$$\beta_i = \begin{cases} 0 & t_{start} < i < t_{end} \\ 1 & \text{otherwise} \end{cases}$$

$$t_{off} > 4$$

$$t_{start} \sim U(0, 23 - t_{off})$$

$$\Delta t \sim U(t_{off}, 24)$$

$$t_{end} = t_{start} + \Delta t$$

$$Theft3(x_i) = \gamma_i x_i \quad \gamma_i \sim U(0.1, 0.8), i = 1, 2, \ldots, 24$$

$$Theft4(x_i) = \gamma_i \bar{x} \quad \gamma_i \sim U(0.1, 0.8), i = 1, 2, \ldots, 24$$

$$Theft5(x_i) = \bar{x} \quad i = 1, 2, \ldots, 24$$

$$Theft6(x_i) = x_{24-i+1} \quad i = 1, 2, \ldots, 24$$

The different theft types can be explained as follows.

Theft Type 1 is reducing of electricity every hour.

Theft Type 2 manipulates electricity consumption and drops to zero in a certain time.

Theft Type 3 is almost similar to theft Type 1 but the number randomly changes hourly.

Theft Type 4 makes electricity consumption per hour less than the mean consumption.

Theft Type 5 modifies electricity consumption per hour to equal the mean consumption.

Theft Type 6 reverses the order of consumption.

Fig. 5 shows an example theft-detection graph. The solid line represents the normal electricity consumption without manipulation and the dotted line represents fraudulent electricity usage grouped into six types of thefts.

Five classifiers we used to classify electric usage as normal or fraudulent: DT, SVM, KNN, NB, and LR. We calculated the accuracy in all blocks, each consisting of a customer population with their 24-hour electricity usage and identified as electricity theft or not based on their electricity usage pattern. Assuming that we provide five smart meters that use different classifiers for theft detection, from the detection result, we can calculate electricity revenue based on electricity usage under normal or fraud usage. The total electricity revenue in all blocks can be computed as the optimization model in Eq. (3)

$$\max B = \sum_{k=1}^{N_{block}} \left(F_k^{TN} + F_k^{FN} + G_k^{TP} + G_k^{FP} + D_k^{TP} + D_k^{FP}\right) - \sum_{k=1}^{N_{block}} \left(Z^{FN} Q_k^{FN} + Z^{FP} Q_k^{FP}\right) \tag{3}$$

Subject to:

$$O_1 = Decision\_Tree(X, y) \tag{4}$$

$$O_2 = Support\_Vector\_Machine(X, y) \tag{5}$$

$$O_3 = K\_Nearest\_Neighbour(X, y) \tag{6}$$

$$O_4 = Naive\_Bayes(X, y) \tag{7}$$

$$O_5 = Logistic\_Regression(X, y) \tag{8}$$

$$v_{ijk}^{TN} = \begin{cases} 1 & \text{if a targety}_{ik}\text{is normal(0)and an output}O_{ijk}\text{is normal(0)} \quad i = 1, 2, \ldots, N_{cust}, j = 1, 2, 3, 4, 5 \\ 0 & \text{otherwise} \qquad\qquad k = 1, 2, \ldots, N\_block \end{cases} \tag{9}$$

$$v_{ijk}^{TP} = \begin{cases} 1 & \text{if a targety}_{ik}\text{ is fraud(1)and an output}O_{ijk}\text{is fraud(1)} \quad i = 1, 2, \ldots, N_{cust}, j = 1, 2, 3, 4, 5 \\ 0 & \text{otherwise} \qquad\qquad k = 1, 2, \ldots, N\_block \end{cases} \tag{10}$$

$$v_{ijk}^{FN} = \begin{cases} 1 & \text{if a target }\ y_{ik}\text{is fraud(1)and an output}O_{ijk}\text{is normal(0)} \quad i = 1, 2, \ldots, N_{cust}, j = 1, 2, 3, 4, 5 \\ 0 & \text{otherwise} \qquad\qquad k = 1, 2, \ldots, N\_block \end{cases} \tag{11}$$

$$v_{ijk}^{FP} = \begin{cases} 1 & \text{if a targety}_{ik}\text{ is normal(0)and an output}O_{ijk}\text{is fraud(1)} \quad i = 1, 2, \ldots, N_{cust}, j = 1, 2, 3, 4, 5 \\ 0 & \text{otherwise} \qquad\qquad k = 1, 2, \ldots, N\_block \end{cases} \tag{12}$$

$$c_{jk} = \begin{cases} 1 & \text{if classifier}j\text{is selected in block}k \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

$$\sum_{j=1}^{5} c_{jk} = 1 \quad k = 1, 2, \ldots, N_{block} \tag{14}$$

Table 6
Interruption cost with certain reliability.

Reliability	Info	Number of customer	Number of customer affected	Total Duration (hour)	SAIFI	SAIDI	CAIDI	Interruption Cost (Pounds)
20 %	Sum	1499	1499	25245	30.00	504.90	504.90	312914.30
	Average	49.97	49.97	841.50	1.00	16.83	16.83	10430.48
	St. Dev.	0.19	0.19	15.70	0.00	0.31	0.31	194.59
	Min	49	49	804	1.00	16.08	16.08	9965.66
	Max	50	50	870	1.00	17.40	17.40	10783.74
50 %	Sum	1499	1499	18047	30.00	360.94	360.94	221182.09
	Average	49.97	49.97	601.70	1.00	12.03	12.03	7372.74
	St. Dev.	0.19	0.19	13.80	0.00	0.28	0.28	201.66
	Min	49	49	578	1.00	11.56	11.56	6994.89
	Max	50	50	636	1.00	12.72	12.72	7823.67
80 %	Sum	1499	1499	8165	30.00	163.30	163.30	46738.19
	Average	49.97	49.97	272.20	1.00	5.44	5.44	1557.94
	St. Dev.	0.19	0.19	11.90	0.00	0.24	0.24	231.12
	Min	49	49	253	1.00	5.06	5.06	1138.86
	Max	50	50	295	1.00	5.90	5.90	1983.99
100 %	Sum	1499	48	283	0.96	5.66	122.42	2257.69
(original data)	Average	49.97	1.6	9.43	0.03	0.19	4.08	75.26
	St. Dev.	0.19	1.40	11.10	0.03	0.22	4.57	113.03
	Min	49	0	0	0.00	0.00	0.00	0.00
	Max	50	5	44	0.10	0.88	19.00	417.64

Table 7
Classification performance and electricity revenue with certain reliability.

Reliability	Info	$N_{customer}$	Σ TN	Σ FP	Σ FN	Σ TP	Electricity Revenue (Pounds)
20 %	Sum	1499	754	249	252	244	198241.33
	Average	49.97	25.13	8.30	8.40	8.13	6608.04
	St. Dev.	0.19	8.19	6.23	4.08	5.64	1367.14
	Min	49	8	0	1	2	4495.06
	Max	50	38	22	15	25	9721.19
50 %	Sum	1499	857	146	244	252	317288.13
	Average	49.97	28.57	4.87	8.13	8.4	10576.27
	St. Dev.	0.19	5.22	2.96	2.54	4.47	1840.53
	Min	49	14	1	4	2	7291.24
	Max	50	38	13	13	22	13831.00
80 %	Sum	1499	927	76	133	363	495358.81
	Average	49.97	30.9	2.53	4.43	12.1	16511.96
	St. Dev.	0.19	4.53	1.91	2.36	4.06	3090.71
	Min	49	16	0	0	6	12231.72
	Max	50	38	7	12	27	22948.40
100 % (original data)	Sum	1499	967	36	88	408	598391.84
	Average	49.97	32.23	1.2	2.93	13.6	19946.40
	St. Dev.	0.19	3.81	1.13	1.95	4.01	4061.55
	Min	49	20	0	0	7	13622.96
	Max	50	38	4	10	27	28553.05

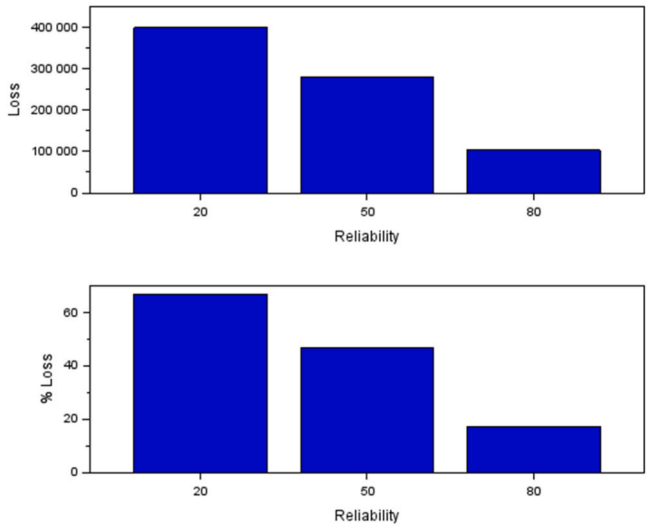

Fig. 8. The loss percentage by different transformer reliability.

$$C_k^{TN} = v_{ijk}^{TN} c_{jk} \quad k = 1, 2, ..., N_{block} \tag{15}$$

$$C_k^{TP} = v_{ijk}^{TP} c_{jk} \quad k = 1, 2, ..., N_{block} \tag{16}$$

$$C_k^{FN} = v_{ijk}^{FN} c_{jk} \quad k = 1, 2, ..., N_{block} \tag{17}$$

$$C_k^{FP} = v_{ijk}^{FP} c_{jk} \quad k = 1, 2, ..., N_{block} \tag{18}$$

$$F_k^{TN} = \sum_{t=1}^{24} \sum\nolimits_{i \in C_k^{TN}} f_{itk} p_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{19}$$

$$F_k^{FN} = \sum_{t=1}^{24} \sum\nolimits_{i \in C_k^{FN}} f_{itk} p_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{20}$$

$$G_k^{TP} = \sum_{t=1}^{24} \sum\nolimits_{i \in C_k^{TP}} g_{itk} p_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{21}$$

$$G_k^{FP} = \sum_{t=1}^{24} \sum\nolimits_{i \in C_k^{FP}} g_{itk} p_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{22}$$

$$D_k^{TP} = \sum_{t=1}^{24} \sum_{i \in C_k^{TP}} ((f_{itk} - g_{itk}) p_{ik} + d_{ik}) \quad k = 1, 2, \ldots, N_{block} \tag{23}$$

$$D_k^{FP} = \sum_{t=1}^{24} \sum_{i \in C_k^{FP}} (f_{itk} - g_{itk}) p_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{24}$$

$$Q_k^{FN} = \sum_{i \in C_k^{FN}} q_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{25}$$

$$Q_k^{FP} = \sum_{i \in C_k^{FP}} q_{ik} \quad k = 1, 2, \ldots, N_{block} \tag{26}$$

Decision variables v_{ijk}^{TN} are binary when the target is normal and the output is normal in the i-th customer at block k using the j-th classifier, v_{ijk}^{TP} are binary variables when the target is fraud and the output is fraud in the i-th customer at block k using the j-th classifier, v_{ijk}^{FN} are binary variables when the target is fraud and the output is normal in the i-th customer at block k using the j-th classifier, v_{ijk}^{FP} are binary variables when the target is normal and the output is fraud in the i-th customer at block k using the j-th classifier, and c_{jk} is the selected classifier method in block k.

$$v_{ijk}^{TN}, v_{ijk}^{TP}, v_{ijk}^{FN}, v_{ijk}^{FP} \in \{0,1\} \quad i = 1,2,\ldots,N_{cust}, j = 1,2,3,4,5, k = 1,2,\ldots,N_{block}$$

$$c_{jk} \in \{0,1\} \quad k = 1,2,\ldots,N_{block}, j = 1,2,3,4,5$$

The constraints in Eqs. (4)–(8) represent the classification output when the smart meter is using the DT, SVM, KNN, NB, and LR in Eqs. (4), (5), (6), (7), and (8), respectively.

The classification output for each classifier is compared with the target dataset. Variables in Eq. (9) are binary when the target is normal and the output is normal in the i-th customer using the j-th classifier, variables in Eq. (10) are binary when the target is fraud and the output is fraud in the i-th customer using the j-th classifier, variables in Eq. (11) are binary when the target is fraud and the output is normal in the i-th customer using the j-th classifier, and variables in Eq. (12) binary when the target is normal and the output is fraud in the i-th customer using the j-th classifier. The variables of Eq. (13) are binary variables of the selected classifier and in Eq. (14) only a classifier is selected for each block.

For each block, we cluster customers inC_k^{TN}as a customer cluster where their normal usage is labeled as normal usage at block $k$as in Eq.

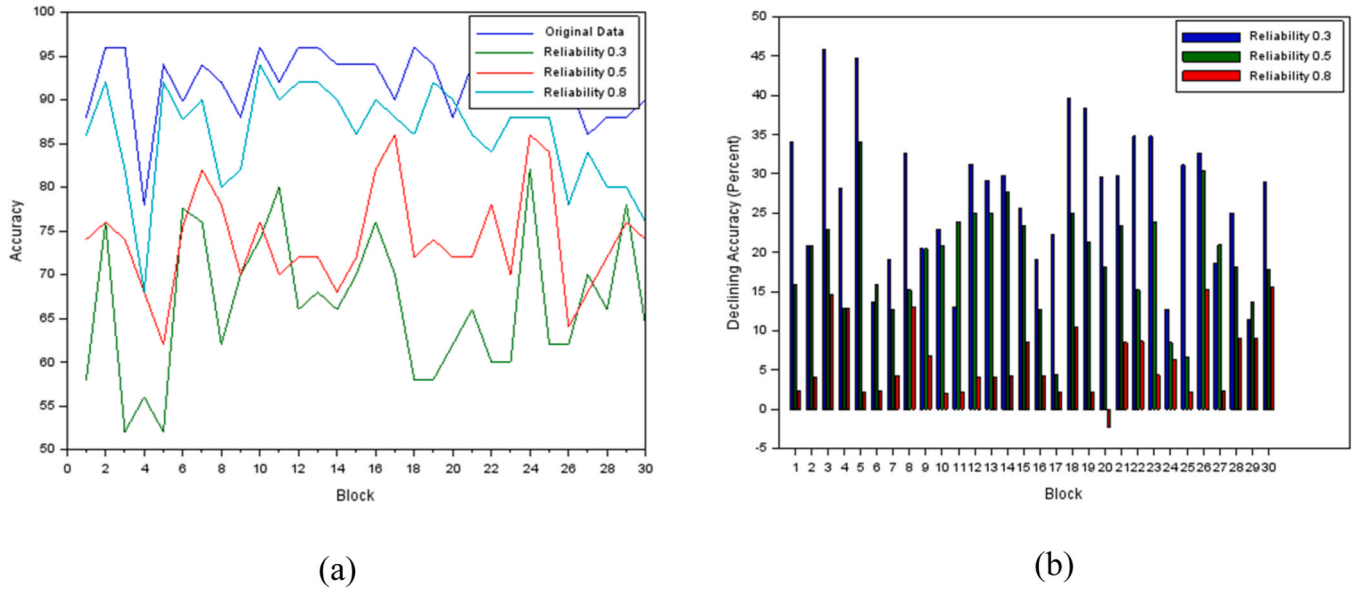

Fig. 9. The effect of reliability transformer to accuracy. (a) The comparison of accuracy from original dataset and modified dataset (b) Percentage of declining accuracy.

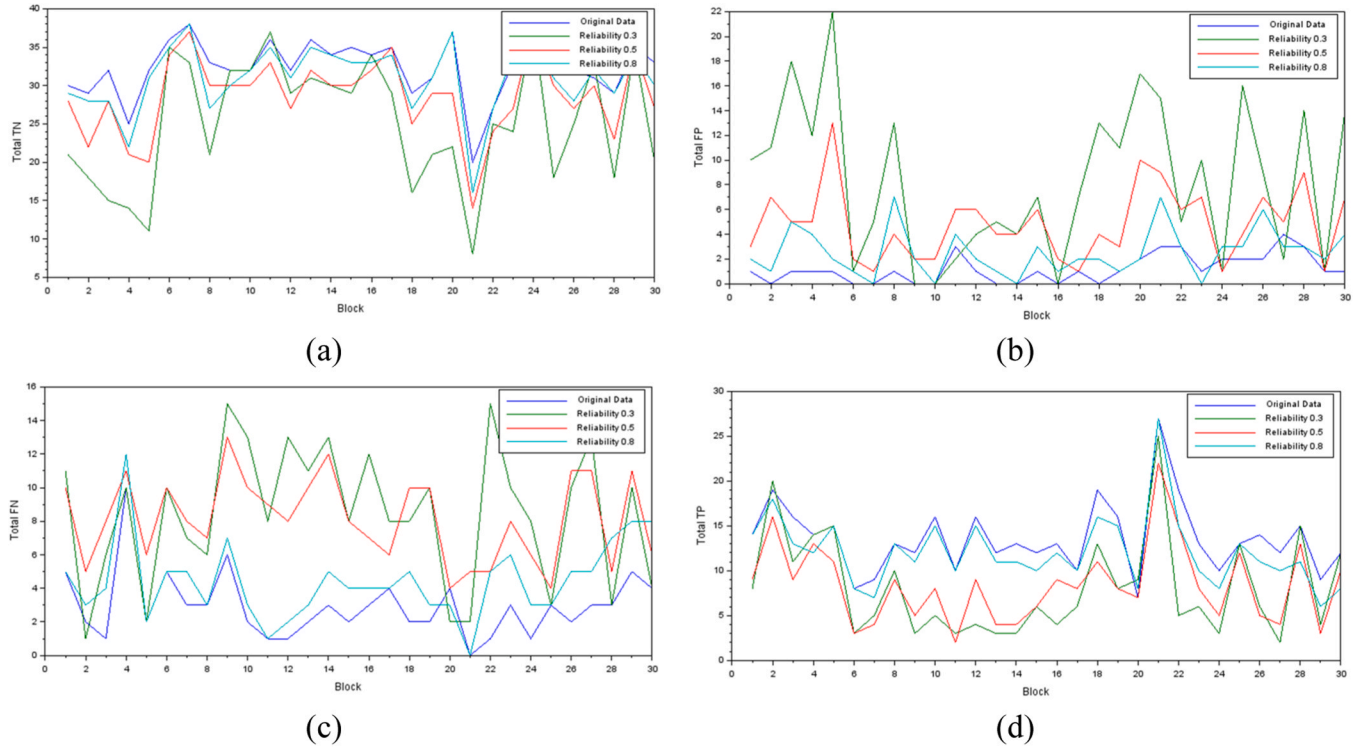

Fig. 10. True classification and false classification of original dataset and modified dataset by certain reliability rate (a) Total of true negative (b) Total of false positive(c) Total of false negative (d) Total of true positive.

(15), C_k^{TP} as a customer cluster where their fraud usage is labeled as fraud usage at block k as in Eq. (16), C_k^{FN} as customer cluster where their fraud usage is labeled as normal usage at block k as in Eq. (17), and C_k^{FP} as customer cluster where their normal usage is labeled as fraud usage at block k as in Eq. (18).

The electricity usages f_{itk} and g_{itk} are normal and fraudulent, respectively in block k, customer i, at time t. Eqs. (19) and (20) represent the electricity revenue using normal usage with unmodified load usage for 24 hours in the electricity bill. Those cases occur in customer cluster C_k^{TN} in Eq. (19) and customer cluster C_k^{FN} in Eq. (20). Eqs. (21) and (22) represent the electricity revenue using fraud usage with modified load usage for 24 hours. Those cases occur in customer cluster C_k^{TP} in Eq. (19) and customer cluster C_k^{FP} in Eq. (20).

For the electricity price, p_{ik} is the electricity price per kWh for block k, customer i.The unpaid electricity price by block k, customer$i$, time t is $(f_{ijk} - g_{ijk})$ and d_{ik} are the fines imposed on block k, customer i when their theft is detected correctly. q_{ik} is the repairing cost for the detector that misclassify in block k, customer$i$. Eq. (23) calculates the unpaid

Table 8
Statistical analysis of transformer reliability.

Reliability	P-Value	Conclusion
Reliability 20 %	0.000	Significant. Accuracy with transformer reliability 20 % is decreasing
Reliability 50 %	0.000	Significant. Accuracy with transformer reliability 50 % is decreasing
Reliability 80 %	0.000	Significant. Accuracy with transformer reliability 80 % is decreasing

electricity price and fines imposed on customer cluster C_k^{TP}, and Eq. (24) calculates the unpaid electricity by customer cluster C_k^{FP}. The repairing costs due to misclassification are allocated to customer cluster C_k^{FN}in Eq. (25) and customer cluster C_k^{FP}in Eq. (26) with Z^{FN} and Z^{FP} being the penalty terms due to misclassifying either *FN* or *FP*.

4.2. Integration to interruption

Interruptions sometimes occur in power distribution networks, where service to one or more customers, which can cause lost of power. They are caused by component outages. Customers incur interruption costs, which include the cost of production loss during interruption. The distribution system performance of power distribution networks is evaluated using reliability indexes such as system average interruption frequency index (SAIFI), system average interruption duration index (SAIDI), and customer average interruption duration index (CAIDI). SAIFI is the proportion of the number of customers encountering interruption, SAIDI is the comparison of interruption duration with the number of customers, and CAIDI is the rasio between SAIDI and CAIDI. For computing these indexes, we determine n_{ik} where it equals 1 when there is no electricity supply in customer i, block k at any time t causing electricity usage f_{itk} equals 0 kW, as in Eq. (27).

$$n_{ik}=\begin{cases}1 & \text{if} f_{itk}=0, t\in\{1,2,\ldots,24\}\\ 0 & \text{otherwise}\end{cases} \quad i=1,2,\ldots,N_{cust}, k=1,2,\ldots,N_{block} \tag{27}$$

The formulas for calculating SAIFI, SAIDI, and CAIDI for each block can be seen in Eq. (28), Eq. (29), Eq. (30), respectively.

$$SAIFI(k)=\frac{\text{total number of customer interruption}}{\text{total number of customer served}}=\frac{\sum_{i=1}^{N_{cust}} n_{ik}}{N_{cust}} \quad k=1,2,\ldots,N_{block} \tag{28}$$

$$SAIDI(k)=\frac{\text{total duration of customer interruption}}{\text{total number of customer served}}=\frac{\sum_{i=1}^{N_{cust}} r_{ik}n_{ik}}{N_{cust}} \quad k=1,2,\ldots,N_{block} \tag{29}$$

$$CAIDI(k)=\frac{\text{total duration of customer interruption}}{\text{total number of customer interruption}}=\frac{\sum_{i=1}^{N_{cust}} r_{ik}n_{ik}}{\sum_{i=1}^{N_{cust}} n_{ik}} \quad k=1,2,\ldots,N_{block} \tag{30}$$

where r_{ik} is the duration of interruption (hour) at customer i, block k.

Interruption costs depend on the type of customer, such as residential (R), agricultural (A), commercial (C), industrial (I), or public (P). Additionally, various costs accrue according to the duration of the interruption, measured in kWh. The longer the duration of interruption, the more the costs. The interruption cost can be computed as in Eq. (31)

$$IC=\sum_{k=1}^{N_{block}}\left(\sum_{i\in U_R} I^R r_{ik}+\sum_{i\in U_C} I^C r_{ik}+\sum_{i\in U_A} I^A r_{ik}+\sum_{i\in U_I} I^I r_{ik}+\sum_{i\in U_P} I^P r_{ik}\right) \tag{31}$$

The parameters are described as follows:
U_R: The set of residential customers
U_C: The set of commercial customers
U_A: The set of agricultural customers
U_I: The set of industrial customers
U_P: The set of public customers
I^R: Interruption cost in pounds per hour for residential customers
I^C: Interruption cost in pounds per hour for commercial customers
I^A: Interruption cost in pounds per hour for agricultural customers
I^I: Interruption cost in pounds per hour for industrial customers
I^P: Interruption cost in pounds per hour for public sector customers
r_{ik}: Interruption duration for block k customer i(hour)

Therefore, there are two objectives in Eq. (3) and Eq. (31). Becauseobjective in Eq. (3) is about power plant revenue and objective on Eq. (31) is about customer interruption cost, then weight factor w are inserted for converting customer losses weighted to power plant. By integrating the interruption cases, the objective function in Eq. (3), can be modified by subtracting interruption cost from electricity revenue as in Eq. (32).

$$\max B-\sum_{i=1}^{N_{block}}\left(w_1\sum_{j\in C_R} I^R r_{ij}+w_2\sum_{j\in C_C} I^C r_{ij}+w_3\sum_{j\in C_A} I^A r_{ij}+w_4\sum_{j\in C_I} I^I r_{ij}+w_5\sum_{j\in C_P} I^P r_{ij}\right) \tag{32}$$

where w_1, w_2, w_3, w_4, w_5 are the weight factors corresponding to the interruption costs for residential, commercial, agriculture, industrial, and public sector customers weighted to power plant, respectively.

5. Numerical results

The simulation data are open source from Kaggle (Smart meters in London (kaggle.com)). The data were taken from smart meters in every home in England, Wales, and Scotland. There are 112 blocks in the dataset; however, we used a subset of data containing 30 blocks. Each block has an average of 31243 entries, and electricity usages were measured half-hourly making 48 columns. From each block, every ID had records consisting of daily electricity usage. We used a unique ID parameter so that each column consisted of 50 homes as customers on average. For each customer, electricity usage was changed hourly data so that there were 24 columns. The simulations were run in Python programming that implements machine-learning techniques.

First, for each block, theft detection was classified using five different classification methods: DT, SVM, KNN, NB, and LR. Their average accuracies were compared with the aggregated dataset. Second, we

Table 9
Profit of power plant with certain reliability.

Reliability	Info	$N_{customer}$	Electricity Revenue (Pounds)	Interruption Cost (Pounds)	Revenue (Pounds)
20 %	Sum	1499	198241.33	312914.30	−114672.97
	Average	49.97	6608.04	10430.48	−3822.43
	St. Dev.	0.19	1367.14	194.59	1445.35
	Min	49	4495.06	9965.66	−6226.70
	Max	50	9721.19	10783.74	−492.37
50 %	Sum	1499	317288.13	221182.09	96106.04
	Average	49.97	10576.27	7372.74	3203.54
	St. Dev.	0.19	1840.53	201.66	1796.04
	Min	49	7291.24	6994.89	−10.44
	Max	50	13831	7823.67	6198.33
80 %	Sum	1499	495358.81	46738.19	448620.62
	Average	49.97	16511.96	1557.94	14954.02
	St. Dev.	0.19	3090.71	231.12	3105.89
	Min	49	12231.72	1138.86	10742.77
	Max	50	22948.40	1983.99	21581.82
100 % (original data)	Sum	1499	598391.84	2257.69	596134.15
	Average	49.97	19946.40	75.26	19871.14
	St. Dev.	0.19	4061.55	113.03	4099.60
	Min	49	13622.96	0	13435.05
	Max	50	28553.05	417.64	28553.05

selected the best classifier, with the best average accuracies. Then, we modified the dataset by adding interruption data according to the reliability rate. From the modified dataset with interruption data, we observed the effects of reliability rate on interruption cost, true and false theft prediction, and electricity revenue.

From previous studies done by Zidi et al., (2023) using KNN, DT, RF, Bagging, and ANN and by Jokar et al. (2016) using SVM, their accuracy can be seen in Table 2. Their results showed the better accuracy results because the number of training data is very huge. The more training process would give the better accuracy. Because they utilized large number of instances for training process, the time consumed was longer rather than this study.

For the comparison with this study, we do undersampling to be 50 instances as our experiments. The accuracies of undersampling are around neighbourhood our accuracies we experimented.

5.1. The effect of aggregated parameters to electricity theft detection

Six types of theft were defined according to their manipulation of smart meter readings. However, in this simulation, we used a single classification, that is, normal usage (0) and fraud (1). We divided the dataset into 70 % normal hourly electricity usage and 30 % fraud hourly electricity usage. The classification methods used for theft detection are DT, SVM, KNN, NB, and LR

For each block, we split the dataset into 70 % for training and 30 % for testing. We classified the dataset using different variables. In the first experiment, we used the original hourly data, thus each row had 24 columns. In the second, third, fourth, and fifth experiments, we aggregated the times to two-, four-, six-, and twelve-hour data, respectively. Therefore, we simplified the columns to 12, 6, 4, and 2 columns in the second, third, fourth, and fifth experiments, respectively.

For each block, we calculated the average accuracy for each experiment. The average accuracy was obtained from the accuracies of each of the five classification methods. The results are shown in Fig. 6(a)-(d). Higher accuracies were obtained when the dataset parameters were aggregated in the third experiment as shown in Fig. 6(b); the time was aggregated to four-hour data. This is because the size of the dataset N_{cust} is quite small—50 customers in each block. However, when parameters are too small, as in the fifth experiment (Fig. 6(d)), by aggregating the time to twelve-hour data, two parameters are left and the input data is insufficient for training. The improvement accuracy of aggregated parameters compared with actual parameters per hour data are computed in Eq. (33).

$$\text{Percent Improvement} = \frac{\sum_{i=1}^{N} (\text{Aggregated Accuracy}(i) - \text{Original Accuracy}(i))}{\sum_{i=1}^{N} \text{Original Accuracy}\ (i)} \times 100\% \tag{33}$$

The percent improvement on Eq. (33) can be either positive or negative depend on the numerator. When numerator is positive, it means that aggegated accuracy is better than original accuracy that impact the positive improvement, vice versa.

The accuracy results from Experiment 1 (using hourly data), Experiment 2 (using two-hour data), Experiment 3 (using four-hour data), Experiment 4 (using six-hour data), and Experiment 5 (using twelve-hour data) can be seen in Table 3.

Table 3 shows that Experiment 3 achieved the best accuracy of all experiments by accuracy mean of five different classifiers are 75.818 percent and made improvement of 11.435 percent of using actual data. Consequently, we used Experiment 3 data for computing electricity revenue for each block.

For observing the significance of aggregating parameters in making electricity theft detection accuracy in experiment 2, experiment 3, experiment 4, experiment 5 with experiment 1 by original hourly data, the Paired Sampled T-Test with significance level $\alpha = 0.05$ is applied and the results are in Table 4. From the Table 4,we conclude that aggregating parameters can affect electricity theft detection accuracy.

5.2. The effect of reliability factor and interruption to electricity theft detection

Assuming that transformers are reliable in distributing electricity to homes, the 24-hour electricity usage in kW is shown in Fig. 6.

The performance of transformers in distributing electricity depends on their reliability. When reliable, they minimize electricity interruption. When an interruption occurs, the data shows 0 kW in the time interval, meaning no electricity was supplied to homes as in Fig. 7.

We experimented with transformers of varying reliability to determine the impact of the reliability factor on interruption costs, which depend on customer type and interruption duration. Surveys were done to estimate the interruption loss per kWh. The interruption costs are presented in Table 5 (Dezaki et al., 2015).

Interruption costs are also affected by the reliability of transformers in distributing electricity. The higher the reliability, the lower the interruption costs. In this study, we varied the reliability rate: 20 %, 50 %, 80 %, and 100 % from the original data. From the original dataset, we calculated SAIFI, SAIDI, CAIDI, and interruption cost as in Table 3. In the experiments, suppose that f_{ijk} is the electricity usage in kW for customer j in block i at time k and R is the reliability factor. The modification can be done by generating a random number r uniformly distributed between 0 and 1 since the interruption can occur in any time as in Eq. (34)

$$f_{itk} = \begin{cases} f_{itk} & if r \le R \\ 0 & otherwise \end{cases} \quad i = 1, 2, .., N_{cust}, t = 1, 2, \ldots, 24, k = 1, 2, \ldots, N_{block} \tag{34}$$

The total interruption cost affected by reliability rates of 20 %, 50 %, 80 %, and 100 % from the original data can be seen in Table 6. The dataset information consisting of sum, average, standard deviation, minimum, and maximum are derived from electricity usage data from 30 blocks and each block contains 50 customers.

From Table 6, we can conclude that when the reliability of the transformer is small (for example, 20 %), the average interruption cost can increase by 10430.48 pounds. On the other hand, when the transformers are reliable, an uninterrupted electricity supply results in minimal interruption costs.

We investigated the effect of transformer reliability on the performance of electricity theft detection. ΣTN is the number of customer clusters with normal usage that are correctly detected as normal usage. ΣFP is the number of customer clusters with normal usage that are incorrectly detected as fraud usage. In this case, the detector may be malfunctioning. They only pay the unpaid electricity price and the power supplier incurs repairing costs. ΣFN is the number of customer clusters with fraud usage that are incorrectly detected as normal usage. ΣTP is the number of customer clusters with fraud usage that are correctly detected as fraud usage, or in other words, their illegal behavior is identified, and they must pay fines and unpaid electricity.

When a certain percent of reliability is applied, electricity usage interruption occurs. Table 7 shows the effects of 20 %, 50 %, 80 %, and 100 % reliability from original data on the classification performance and the impact on electricity revenue. Low reliability causes frequent interruptions, affecting the classification performance, based on which electricity revenue is calculated. Faulty classification (cluster *ΣFP* and*ΣFN)* results in repairing costs.

Fig. 8 describe about amount of loss when transformer reliabilities are employed. The lower reliability of transformer impacts to higher loss of electricity revenue because any interruptions are frequently occur and no electricity revenue when interruptions.

Fig. 9(a) shows the comparison of accuracy from the original dataset and dataset with reliabilities 20 %, 50 %, 80 %, and 100 % from the original data, and Fig. 10(a)-(d) show detailed classification information consisting of true classification (ΣTN andΣTP) and false classification (ΣFP andΣFN). Higher accuracy was achieved on the original dataset, with no modification in the interruption data. Reliability factors affect classification performance; when the transformers have high reliability, electricity is supplied with few interruptions. Datasets with few interruptions are easier to classify. An example is a time interval where electricity usage is 0 kW; with no theft action, the data is still 0 kW and it is classified as normal usage. When theft occurs in scenarios 1, 2, and 3, the data is 0 kW and it is classified as fraud usage. These cause ambiguous output on the training process and low accuracy.The Fig. 9(b) represents percentage of declining accuracy by different reliability factors by Eq. (35).The percent declining accuracy on Eq. (35) can be either positive or negative depend on the numerator. When numerator is positive, it means that accuracy by reliability is better than original accuracy, vice versa. From the Fig. 9(b), it can see that only at the block 20, accuracy by reliability 80 % is better than original accuracy.

$$\%Declining\ Accuracy = \frac{\sum_{i=1}^{N} (Original\ Accuracy(i) - Accuracy\ by\ Reliability(i))}{\sum_{i=1}^{N} Original\ Accuracy(i)} \times 100\% \tag{35}$$

For observing the significance of transformer reliability in making electricity theft detection accuracy compared with transformer reliability 100 %, the Paired Sampled T-Test with significance level α= 0.05 is applied and the results are as Table 8. From the Table 8, we can conclude that all transformer reliabilities affect electricity theft detection accuracy.

For each block, we can compute the revenue of the power plant as the function of electricity revenue and interruption cost, where w_i is the weight of the interruption cost block i using *Eq. (26)*.

Table 9 shows the power plant profit at different reliability rates. Low reliability leads to smaller profit because of higher interruption costs. When the reliability is 20 %, the interruption cost is very large because there are many interruptions shown by 0 kW in electricity usage. The consumption values of 0 kW in any time do not contribute to electricity revenue.

6. Conclusions

The electricity theft-detection model is a development of the machine-learning problem of maximizing accuracy, especially in fraud detection. Five classifiers methods DT, SVM, KNN, NB, LR have been applied with the aggregated parameters. Accuracy is optimal when misclassifications are few (false negative and false positive) and the numbers of true negative and true positive are high. Aggregating parameter inputs can improve model accuracy. The reliability factor represents interruptions in electricity usage. A small reliability factor results in high interruption costs and low profit for the power plant. It also affects electricity theft detection performances.

Our findings indicate that using optimal aggregated parameters significantly enhances detection accuracy 10.709 percent, 11.435 percent, 4.909 percent, and 2.097 percent from original parameters

depend on the number of aggregation in 2-hour, 4-hour, 6-hour, and 12-hour, respectively.

The lower transformer reliability leads to increased loss with percentage 66.87 percent, 46.98 percent, 17.22 percent and reduced theft-detection efficiency by 27.32 percent, 19.23 percent, 6.20 percent depend on the reliability factor, 20 percent, 50 percent, and 80 percent, respectively.

Based on our findings, these can give suggestions to the power company to maintain the transformer regularly considering that there is a significant impact such as declining income if an interruption occurs. Moreover, the quality of smart meter is also considered to create the best accuracy and avoid misclassification.The maintenances of smart meter also should be done since they can prevent the electricity theft and avoid the expensive repairing cost or purchasing cost when they are broken.

Subject to the availability of huge amounts of data, our future research will apply deep-learning algorithms such as CNN to handle the data, which is expected to produce good accuracy in theft detection. Besides time-series parameter inputs, we may develop other features in electricity theft detection to produce optimal performance.

CRediT authorship contribution statement

Dinita Rahmalia: Writing – original draft, Validation, Methodology, Data curation, Conceptualization. **Yu-Chung Tsao:** Writing – review & editing, Writing – original draft, Validation, Supervision, Methodology, Conceptualization. **Jye-Chyi Lu:** Writing – review & editing, Supervision, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Data will be made available on request.

Acknowledgements

This paper is supported in part by the National Science and Technology Council, Taiwan under grant 113-2628-E-011-009 and grand 113-2221-E-011-129; the National Taiwan University of Science and Technology under grant NTUST- DROXO TECH- No. 10050.

Appendix

Decision tree

The classification method of Decision Tree is tree construction consisting of root at the top of tree, some branches, and leaf node at the bottom of tree as in Fig. 11. Each leaf node is used to make decision output i.e. 'Yes' represented by 1 or 'No' represented by 0. In the path of tree, there are some rectangle boxes consisting of parameter to take decision satisfying or not.

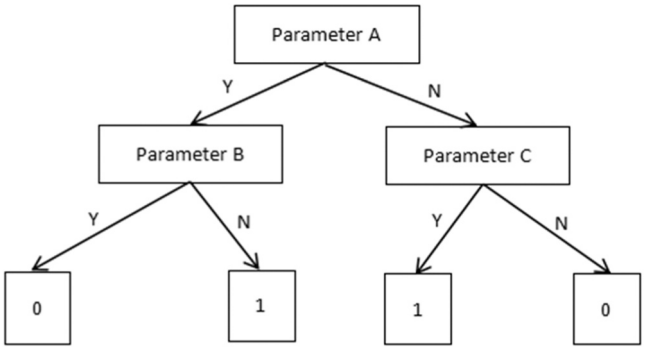

Fig. 11. Decision Tree

Suppose that the input parameters $X_i = (x_{i1}, x_{i2}, \ldots, x_{i,N_{input}}), i = 1, 2, \ldots, N_{data}$ and targets$y_i \in \{0, 1\}, i = 1, 2, \ldots, N_{data}$. The algorithm for determining output of Decision Tree $O_i^{DT}, i = 1, 2, \ldots, N_{data}$ are $Decision\_Tree(X, y)$ by computing Entropy and Information Gain (IG) as follows:

$$Entropy(S) = \sum_{c=0}^{N_{class}} -\frac{y_c}{\sum_c y_c} \log_2 \left(\frac{y_c}{\sum_c y_c} \right)$$

Where $\boldsymbol{y_c}$is the total number of class c at the training target and $\boldsymbol{N_{class}}$ is the the number of classes on training target. We note that when we only do simple classification 'Yes' notated by 1 or 'No' notated by 0, we set $\boldsymbol{N_{class} = 1}$.

$$\boldsymbol{IG(S, X_d) = Entropy(S) - \sum_{c=0}^{N_{X_d.class}} \left(\frac{S_{X_d \in c}}{S} \times Entropy\left(S_{X_d \in c}\right) \right) \quad d = 1, 2, \ldots, N_{input}}$$

With $\boldsymbol{N_{X_d.class}}$ is the number of classes on parameter input $\boldsymbol{X_d}$

Since the model uses simple classification, the output is $\boldsymbol{O_i^{DT} \in \{0, 1\}, i = 1, 2, \ldots, N_{data}}$

Support Vector Machine

The concept of Support Vector Machine (SVM) is making the decision boundary or margin m as far away from the data class as in Fig. 12 . In the two dimensional graph, there are two classes and any points at the right class and any points at the wrong class or misclassification.

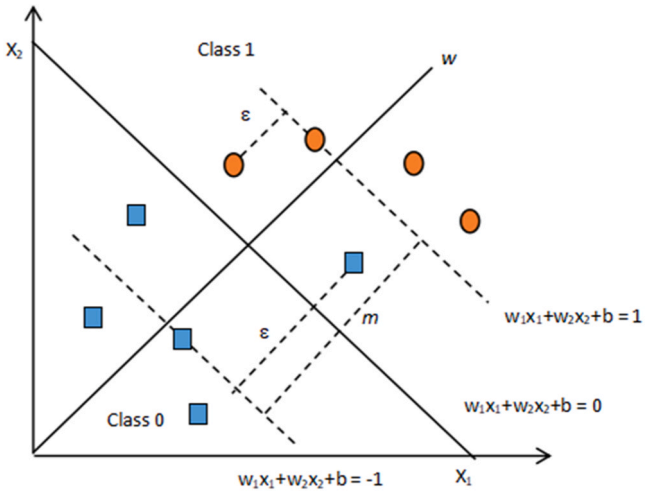

Fig. 12. Support Vector Machine

Suppose margin m is $m = \frac{2}{\|w\|}$, because maximization m similar to minimization $\|w\|$, the input parameters $X_i = (x_{i1}, x_{i2}, \ldots, x_{i,N_{input}}), i = 1, 2, \ldots, N_{data}$ and targets$y_i \in \{0, 1\}, i = 1, 2, \ldots, N_{data}$. The algorithm for determining output of SVM $O_i^{SVM}, i = 1, 2, \ldots, N_{data}$are *Support_Vector_Machine*(X, y).

The optimization of SVM are:

$$\mathbf{min}\frac{\mathbf{1}}{\mathbf{2}}\|\boldsymbol{w}\|^2 + \boldsymbol{C}\sum_{\boldsymbol{i}=\mathbf{1}}^{\boldsymbol{N_{data}}}\boldsymbol{\varepsilon_i}$$

Subject to:

$$\boldsymbol{y_i}\left(\boldsymbol{w^T x_i} + \boldsymbol{b}\right) \geq \mathbf{1} - \boldsymbol{\varepsilon_i} \quad \boldsymbol{i} = \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{N_{data}}$$

$$\varepsilon_i \geq 0 \quad i = 1, 2, \ldots, N_{data}$$

With $w = (w_1, w_2, \ldots, w_{N_{input}})$ are the coefficient of linear equation, b is the constant, ε_i is the error at data point i, and $y_i \in \{-1, 1\}$.

$$O_i^{SVM} = \begin{cases} -1 & if w^T x_i + b \leq 0 \\ 1 & otherwise \end{cases}$$

$$O_i^{SVM} \leftarrow \begin{cases} 0 & if O_i^{SVM} = -1 \\ 1 & otherwise \end{cases}$$

K nearest neighbor

The simple classification method using K-Nearest Neighbor (KNN) is utilizing the distance between two points as in Fig. 13 .

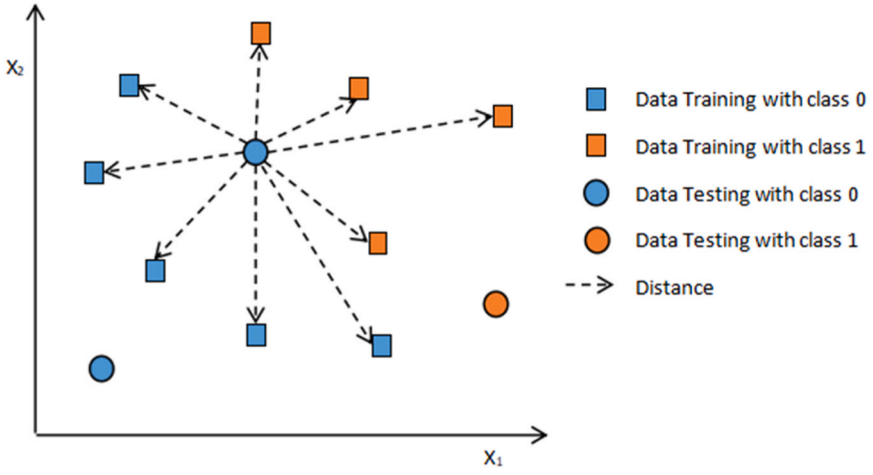

Fig. 13. K-Nearest Neighbor

Generally, the distance between two point $x = (x_1, x_2, \ldots, x_{N_{input}})$ and $y = (y_1, y_2, \ldots, y_{N_{input}})$can be calculated as follows:

$$dist(x,y) = \sqrt{\sum_{i=1}^{N_{input}} (x_i - y_i)^2}$$

Suppose that the input parameters $X_i = (x_{i1}, x_{i2}, \ldots, x_{i,N_{input}}), i = 1, 2, \ldots, N_{data}$ and targets$y_i \in \{0,1\}, i = 1, 2, \ldots, N_{data}$. The algorithm for determining output of K-Nearest Neighbor $O_i^{KNN}, i = 1, 2, \ldots, N_{data}$ are $KNearest\_Neighbor(X,y)$ is by ordering K shortest distances and taking the class with the highest number as output decision of KNN

$$O_i^{KNN} = \underset{c}{argmax}\left(Y_i^{asc}\right) \quad i = 1, 2, \ldots, N_{testing}$$

Naive Bayes

Naive bayes classifier works as Bayes theorem. Each pair of parameter input is assumed independent each other.

The implementation of Naive Bayes method to the classification problem are based conditional probability. Suppose the probability parameter input x_d in class c_d given the probability of target c is:

$$P(x_d \in c_d | y \in c) = \frac{P(x_d \in c_d \cap y \in c)}{P(y \in c)} \qquad d = 1, 2, \ldots, N_{input}, c = 0, \ldots, N_{class}$$

Suppose that the input parameters $X_i = (x_{i1}, x_{i2}, \ldots, x_{i,N_{input}}), i = 1, 2, \ldots, N_{data}$ and targets$y_i \in \{0,1\}, i = 1, 2, \ldots, N_{data}$. The algorithm for determining output of Naive Bayes $O_i^{NB}, i = 1, 2, \ldots, N_{data}$ are $Naive\_Bayes(X,y)$.

For overall parameter inputs, the conditional probability are:

$$P\left(y \in c | x_1 \in c_1, x_2 \in c_2, \ldots, x_{N_{input}} \in c_{N_{input}}\right) = \frac{P\left(x_1 \in c_1 \middle| y \in c\right).P\left(x_2 \in c_2 \middle| y \in c\right)\ldots.P\left(x_{N_{input}} \in c_{N_{input}} \middle| y \in c\right)p\left(y \in c\right)}{p\left(x_1 \in c_1\right).p\left(x_2 \in c_2\right)\ldots.p\left(xN_{input} \in cN_{input}\right)} c = 0, \ldots, N_{class}$$

Then the output decision of Naive Bayes are class with the most number

$$O_i^{NB} = \underset{c}{argmax}\left(P\left(y \in c | x_1 \in c_1, x_2 \in c_2, x_{N_{input}} \in c_{N_{input}}\right), c = 0, \ldots, N_{class}\right) \quad i = 1, 2, .., N_{data}$$

Since we do a simple classification, we set $N_{class} = 1$

Logistic regression

Logistic Regression is the development of linear regression since linear regression has drawback in predicting binary response variable. In *Fig. 14* , it is obvious that there are values fall below 0 and above 1 when predicting binary response variable.

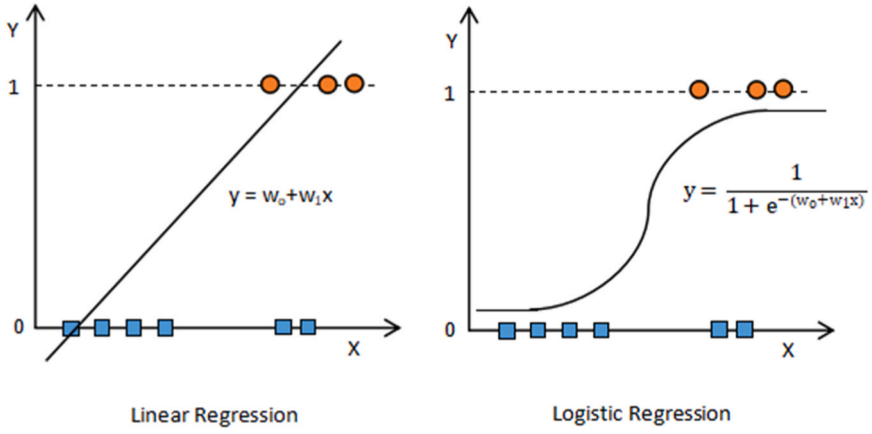

Fig. 14. Linear Regression and Logistic Regression

Suppose that the input parameters $X_i = (x_{i1}, x_{i2}, \ldots, x_{i,N_{input}}), i = 1, 2, \ldots, N_{data}$ and targets$y_i \in \{0,1\}, i = 1, 2, \ldots, N_{data}$. The algorithm for determining output of Logistic Regression $O_i^{LR}, i = 1, 2, \ldots, N_{data}$ are $Logistic\_Regression(X,y)$.

The prediction using Logistic Regression can be constructed as follows:

$$P\left(y = 1 | x_1, x_2, \ldots, x_{N_{input}}\right) = \sigma\left(x_d^T w\right) = \frac{1}{1 + e^{-\left(w_0 + w_1 x_1 + \ldots + w_{N_{input}} x_{N_{input}}\right)}}$$

with $P(y=1|x_1,x_2,...,x_{N_{input}})$ is the probability the class is 1 given parameter inputs $(x_1,x_2,...,x_{N_{input}})$. The output decision of Logistic Regression are:

$$O_i^{LR} = \begin{cases} 1 & \text{if} p_i \geq 0.5 \\ 0 & \text{otherwise} \end{cases} \quad i = 1,2,\ldots,N_{data}$$

References

Achariyakul, N.T., Rerkpreedapong, D., 2022. Optimal preventive maintenance planning for electric power distribution systems using failure rates and game theory. Energies Vol. 15 (No. 14), 5172.

Antaneh, D., Khan, B., Mahela, O.P., Alhelou, H.H., Guerrero, J.M., 2021. Distribution network reliability enhancement and power loss reduction by optimal network reconfiguration. Comput. Electr. Eng. Vol. 96, 107518.

Aschi, M., Bonura, S., Masi, N., Messina, D., Profeta, D., 2022. Cybersecurity and Fraud Detection in Financial Transactions. Big Data and Artificial Intelligence in Digital Finance. Springer, pp. 269–278.

Aslam, F., Hunjra, A.I., Ftiti, Z., Louhichi, W., Shams, T., 2022. Insurance fraud detection: evidence from artificial intelligence and machine learning. Res. Int. Bus. Financ. Vol. 62, 101744.

Bagga, S., Goyal, A., Gupta, N., Goyal, A., 2020. Credit card fraud detection using pipelining and ensemble learning. Preced. Comput. Sci. Vol. 173, 104–112.

Bahnsen, A.C., Aouada, D., Stojanovic, A., Ottersten, B., 2016. Feature engineering strategies for credit card fraud detection. Expert Syst. Appl. Vol. 51, 134–142.

Bai, R., 2024. Image manipulation detection and localization using multi-scale contrasive learning. Appl. Soft Comput. Vol. 163, 111914.

Blaszczynski, J., Filho, A.T.A., Matuszyk, A., Szelag, M., Slowinski, R., 2021. Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. Expert Syst. Appl. Vol. 163, 113740.

Camacho, I.C., Wang, K., 2022. Convolutional neural network initialization approaches for image manipulation detection. Digit. Signal Process. Vol. 122, 103376.

Carcillo, F., Borgne, Y.A.L., Caelen, O., Kessaci, Y., Oble, F., Bontempi, G., 2021. Combining unsupervised and supervised learning on credit card fraud detection. Inf. Sci. Vol. 557, 317–331.

Chen, K., Yadav, A., Khan, A., Zhu, K., 2020. Credit fraud detection based on hybrid scoring model. Procedia Comput. Sci. Vol. 167, 2–8.

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., 2023. Credit card fault detection in the era of disruptive technologies: a systematic review. J. King Saudi Univ. Comput. Inf. Sci. Vol. 35 (No. 1), 145–174.

Chouiekh, A., Haj, E.H., 2018. ConvNets for fraud detection analysis. Procedia Comput. Sci. Vol. 127, 133–138.

Dezaki, H.H., Abyaneh, H.A., Khiavi, H.H., 2015. Reliability optimization of electrical distribution system using interval loops to minimize energy not supplied. J. Appl. Res. Technol. Vol. 13, 416–424.

Fogliatto, M.S.S., Caetano, H.O., Desuo, N., Massignan, J.A.D., Fanucchi, R.Z., London, J. B.A., Pereira, B.R., Bessani, M., Maciel, C.D., 2022. Power distribution system interruption duration model using reliability analysis regression. Electr. Power Syst. Res. Vol. 211, 108193.

Forcan, J., Forcan, M., 2022. Optimal placement of remote-controlled switches in distribution network considering load forecasting. Sustain. Energy Grids Netw. Vol. 30, 100600.

Haq, E.U., Pei, C., Zhang, R., Jianjun, H., Ahmad, F., 2023. Electricity-theft detection for smart grid security using smart meter data: a deep-CNN based approach. Energy Rep. Vol. 9, 634–643.

Hilal, W., Gadsden, S.A., Yawney, J., 2022. Financial fraud. A Rev. Anom. Detect. Tech. Recent Adv. Expert Syst. Appl. Vol. 193, 116429.

Izotova, A., Valiullin, A., 2021. Comparison of poisson process and machine learning algorithms approach for credit card fraud detection. Procedia Comput. Sci. Vol. 186, 721–726.

Jessica, A., Raj, F.V., Sankaran, J., 2023. Credit Card Fraud Detection Using Machine Learning Techniques. 2nd International Conference on VisionTowards Emerging Trends in Communicating and Networking Technologies. IEEE, pp. 1–6.

Jokar, P., Arianpoo, N., Leung, V.C.M., 2016. Electricity theft detection in AMI using customer's consumption patterns. IEEE Trans. Smart Grid Vol. 7 (No. 1), 216–226.

Judge, M.A., Khan, A., Manzoor, A., Khattak, H.A., 2022. Overview of smart grid implementation: frameworks, impact, performance, and challenges. J. Energy Storage Vol. 49, 104056.

Khan, Z.A., Adil, M., Javaid, N., Saqib, M.N., Shafiq, M., Choi, J.G., 2020. Electricity theft detection using supervised learning techniques on smart meter data. Sustainability Vol. 12 (No. 19), 8023.

Khodabandehlou, S., Golpayegani, S.A.H., 2022. Market manipulation detection. A Syst. Lit. Rev. Expert Syst. Appl. Vol. 210, 118330.

Lei, Y.T., Ma, C.Q., Ren, Y.S., Chen, X.Q., Narayan, S., Huynh, A.N.Q., 2023. A distributed deep neural network model for credit card fraud detection. Financ. Res. Lett. Vol. 58, 104547.

Lepolesa, L.J., Achari, S., Cheng, L., 2022. Electricity theft detection in smart grids based on deep neural network. IEEE Access Vol. 10, 39638–39655.

Li, S., Han, Y., Yao, X., Yingchen, S., Wang, J., Zhao, Q., 2019. Electricity theft detection in power grids with deep learning and random forests. J. Electr. Comput. Eng. Vol. 2019.

Liao, W., Zhu, R., Yang, Z., Liu, K., Zhang, B., Zhu, S., Feng, B., 2024. Electricity theft detection using graph construction and graph attention network. IEEE Trans. Ind. Inform. Vol. 20 (No. 4), 5074–5086.

Lin, X., Wang, S., Deng, J., Fu, Y., 2023. Image manipulation detection by multiple tampering traces and edge artifact enhancement. Pattern Recognit. Vol. 133, 109026.

Liu, C., Li, S., Shi, L., 2024. A stock price manipulation detecting model with ensemble learning. Expert Syst. Appl. Vol. 248, 123479.

Louw, Q., Bokoro, P., 2019. An alternative technique for the detection and mitigation of electricity theft in South Africa. SAIEE Afr. Res. J. Vol. 110 (No. 4), 209–216.

Mao, X., Sun, H., Zhu, X., Li, J., 2021. Financial fraud detection using the related-party transaction knowledge graph. Procedia Comput. Sci. Vol. 199, 733–740.

Mohan, T., Praveen, K., 2019. Fraud detection in medial insurance claim with privacy preserving data publishing in TLS-N using blockchain. Adv. Comput. Data Sci. 211–220.

Nalayini, C.M., Katiravan, J., Sathyabama, A.R., Rajasuganya, P.V., Abirami, K., 2023. Identification and detection of credit card frauds using CNN. Appl. Comput. Intell. Manag. Math. 267–280.

Reddy, S.R.B., Kanagala, P., Ravichandran, P., Pulimamidi, R., 2024. Effective fraud detection in E-commerce: leveraging machine learning and big data analytics. Meas. Sens. Vol. 33, 101138.

Roseline, J.F., Naidu, G.B.S.R., Pandi, V.S., Rajasree, S.A., Mageswari, N., 2022. Autonomous credit card fraud detection using machine learning approach. Comput. Electr. Eng. Vol. 102, 108132.

Sadgali, I., Sael, N., Benabbou, F., 2019. Performance of machine learning techniques in the detection of financial fraud. Procedia Comput. Sci. Vol. 148, 45–54.

Sadiq, A.S., Faris, H., Al-Zoubi, A., Mirjalili, S., Ghafoor, K.Z., 2019. Chapter 17 – fraud detection model based on multi-verse extraction approach for smart city applications. Smart Cities Cybersecur. Priv. 241–251.

Samanta, P., Jain, S., 2021. Analysis of perceptual hashing algorithms in image manipulation detection. Procedia Comput. Sci. Vol. 185, 203–212.

Stracqualursi, E., Rosato, A., Lorenzo, G.D., Panella, M., Araneo, R., 2023. Systematic review of energy theft practices and autonomous detection through artificial intelligence methods. Renew. Sustain. Energy Rev. Vol. 184, 113544.

Thakur, R., Rohilla, R., 2020. Recent advances in digital image manipulation detection techniques: a brief review. Forensic Sci. Int. Vol. 312, 110311.

Usberti, F.L., Cavellucci, C., Lyra, C., 2023. Interruption flows for reliability evaluation of distribution networks. Oper. Res. Vol. 24 (No. 4), 1–23.

Vidovic, P.M., Vojnovic, N.R., Strezoski, V.C., 2021. A new power flow for multi-phase distribution network with simultaneous phase interruptions. Electr. Eng. Vol. 104, 473–484.

Wang, X., Xie, H., Tang, L., Chen, C., Bie, Z., 2023. Decentralized privacy-preserving electricity theft detection for distribution system operators. IEEE Trans. Smart Grid Vol. 15 (No. 2), 2179–2190.

Xiao, S., Zhang, Z., Yang, J., Wen, J., Li, Y., 2023. Manipulation detection of key populations under information measurement. Inf. Sci. Vol. 638, 1–13.

Yadav, A., Vishwakarma, D.K., 2023. MRT-net: auto-adaptive weighting of manipulation residuals and texture clues for face manipulation detection. Expert Syst. Appl. Vol. 232, 120898.

Yang, K., Chen, W., Bi, J., Wang, M., Luo, F., 2023. Multi-view broad learning system for electricity theft detection. Appl. Energy Vol. 352, 121914.

Zhao, Z., Liu, G., Liu, Y., 2024. Practical privacy-preserving electricity theft detection for smart grid. IEEE Trans. Smart Grid.

Zidi, S., Mihoub, A., Qaisar, S.M., Krichen, M., Al-Haija, Q.A., 2023. Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. J. King Saud. Univ. Comput. Inf. Sci. Vol. 35 (No. 1), 13–25.

Zulu, C.L., Dzobo, O., 2023. Real-time power theft monitoring and detection system with double connected data capture system. Electr. Eng. Vol. 105, 3065–3083.