Grenze International Journal of Engineering and Technology, June Issue

Review of “Detection and Prevention of Electrical Power Theft by Artificial Intelligence and Machine Learning”

Shabbir Ghadiali[1], Dr Naimish Zaveri[2] and Zahabiyah Ghadiali[3]
[1]Ass. Prof, Department of Electrical Engineering, Sarvajanik College of Engineering & Technology, Surat
Email: shabbir.ghadiali@scet.ac.in
[2]Professor, Department of Electrical Engineering, C. K. Pithawala College of Engineering & Technology, Surat
Email: Naimish.zaveri@ckpcet.ac.in
[3]Student, BE 3rd Year, Department of Mechanical Engineering, S V National Institute of Technology, Surat; 2nd Year, BSc (Programing & Data Science) IIT, Madras
Email: zahabiyahghadiali@gmail.com

***Abstract*—The gradual rise in electricity theft is one of the foremost concerns for the electric power distribution system and the poor economic state of the short voltage consumer side. Power theft encloses faulty meters, electricity theft or billing errors. Moreover, this theft will affect the sincere customers, proficient power supply and increases the power generating station demand. In developing nations, theft detection and dealing with the public became very difficult for utility concerns. Also, it will affect the growth of the developing country. Therefore, the consumers develop metering knowledge with the diverse, novel, innovative developments for prohibited electricity theft. This paper discusses the power theft impact factors and detection methods using Artificial Intelligence (AI) and machine learning. Also, this work provides a literature review on the techniques utilised for power theft detection. Consequently, the performance metrics of these conventional techniques in power theft detection are investigated for configuration of further improvement in electricity theft recognition.**

***Index Terms*— Non-technical loss, Advanced Metering Infrastructure, Artificial Intelligence, Data Science, Machine learning, Power theft detection.**

I. INTRODUCTION

A. Background

The electric power system is always considered one of the most significant and fast-growing infrastructures filed in any country, which gives a massive boost to the GDP and economy of the counties [1]. Since electricity was invented, it has been in continuous operation by industry, domestic consumers, and commercial consumers in their day-to-day life. Over time, power usage and the way to generate power from various sources are also evolved. The practice of transmitting the electric power is also getting significantly improving. The power distribution and transmission costs are considerably enhanced by improving the power system, and large numbers of people are now accessible to the electrical energy. Nowadays, smart girds are evolving in the power system. The smart grids are contained additional instruments for digital communication (i.e., Sensors and smart

Grenze ID: 01.GIJET.8.2.7_3

meters). Adding the smart grid to the conventional power system can operate more than one power source, and bidirectional power transmission is also possible [2], [3]. The smart grid can record the tremendous amount of power distribution and consumption data from the consumer end and the distribution company end. Further, this dataset can be utilised for the data analysis by analysing the power consumption pattern of different consumers. Accordingly, the power generation and transmission can be scheduled, and the power system's additional losses can be analysed.

In the power system transmission and distribution section, there are main two categories of power losses 1) technical losses and 2) due to non-technical losses [4], [5]. When the power is transmitted from the power generating station to the primary supply grid, the girds transmit the power to the various power substations. The city substation distributes the power to end users [4]. During this long process of supplying power from one place to another and utilising and emitters losses due to change in different voltage supply levels and as per the consumer, requirement power is provided. Different consumers have different revetments during this process, and some energies are lost. This loss of control is known as a technical power loss. When in the power grid, the consumer tries to steal the energy by bypassing the electric meters or not paying the full invoice amount, known as non-technical loss in the power system. Power and energy theft are considered non-technical losses[5], which lead to a heavy power loss and are one of the responsible reasons for the power grid balancing.

This type of electricity theft mainly occurs in underdeveloped or developing countries where the local people's standard of living is below average, and electricity rates are not affordable for some people, leading them to steal the electric power[6], [7]. India is one of the developing nations that authoritarian states should take to diminish insufficient and uneven power supply and should pay more attention to enhancing the improvement of this segment [8]. After the vast promotion and majority of people's interest in the cryptocurrency, there has been a rise in the crypto-miner in the western countries and which implies a massive load on the power grid, and the rate of electricity is also higher, which encourages most of the crypto miner to theft the electrical energy from the grids[9].

According to the following research article about the electric power theft done in many developing and well-developed countries:

TABLE I. LOSS OF REVENUES DUE TO ELECTRICITY THEFT IN DIFFERENT COUNTRIES[10]

Countries	Power theft (in %)	Loss in revenue (in USD)
India [11]	~30%	$ 16.2 B
South Africa [12]	~33-35%	$ 20 B
Brazil	~20-30%	$ 4.7B
Bangladesh	~14-15%	$70M
Jamaica	~18%	$75M
Pakistan	~25%	$25B
China	~15%	$65M
Malaysia	20%	$229M
Turkish	15%	$1B
United Kingdom	~15%	$217M
United State of America	~2-3.5%	$1B
Canada	-	$125M

As shown in Table , the survey collected in various research work about the amount of electrical energy was stealing in the countries and how much it costs to the government and the distribution companies. Electricity theft is a central portion of the beneficial losses [13]. However, power theft prevention is a challenge without innovative technologies, and it should continuously monitor the data automatically towards the clouds [9].

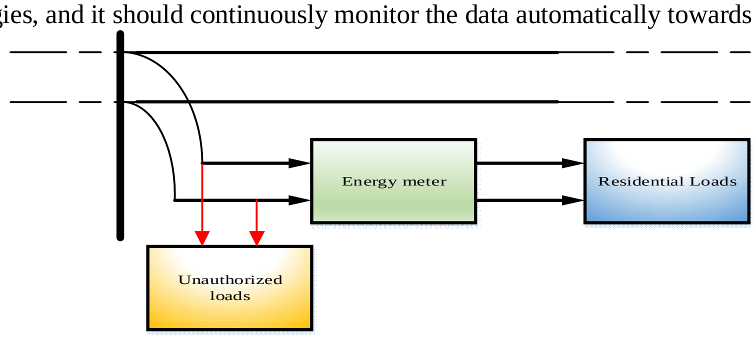

Figure 1shemetic diagram of electric theft of bypassing the electric meters

Mainly, developing countries like India, China, Brazil, Jamaica, and many others majorly face this electricity theft due to higher rate of population increment, higher unemployment rate, lower education, and highly underdeveloped ruler areas. In rural areas, electricity theft is widespread and mainly happens in the distribution lines by rampant hooking [14]. The action in rural areas is not accessible due to the absence of governmental determination [15]. Similarly, the bypass and meter damage are the major problem in the urban sides that is faced by the group of power supply company employees [16]. The Schematic of the Straight tapping in cable for power theft is illustrated in Figure 1. In developing countries like India, power theft is a general consequence. Also, top portions of the power supply are unpaid [17]. Around one-fourth of electricity in India is lost by electricity theft and poor wiring [15], which also can display in Table . The distribution segment, large industries and domestic customers are also spoiled by electricity theft by taking electricity from the grid of national illegally [18]. Electricity theft via meter damage is one of the main problems of commercial loss increases [19]. Each electric component faces these issues at different levels [20]. The power suppliers are continually exposed to new scam methods introduced by innovative persons [21]. The power theft problem also increases because the power supply-demand increases [22]. The low quality of power and income losses because of power theft can create economic problems in the distribution segment. Simultaneously the user experiences common trip issues and voltage variation in the power supplies[17].

B. Motivation

This electricity theft is one of the significant issues and the warring singe for the electric power grid development; There are very high chances that it might surge in the power generation and distribution planning. Also, technical loss in the electrical power system can be easy to recognise and solved by various methods [23]. Still, for this non-technical loss, identification is also one of the challenging aspects because, in every fraud or theft detection condition, most people are honest. So, the task is to identify the fraud consumer from many ethical consumers. Also, as per human rights, it needs to ensure that no honest consumer gets punished, so consumer identification also requires strong evidence [24]. If they caught them, action would be preferable per most countries' rules[25].

In this research study, we analyse and review the various methodologies utilised in the current research work and real-time case studies for the electricity theft detection approaches and the success rate of those methods and the scope of improvements in those approaches.

The paper structure is as follows: the first section is about the introduction of the research paper, including the background of the electricity theft and our motivation for this research purpose; in the following area, we discuss the people's mentality and the mindset based on that information we analysed the reason behind the electricity theft and how government take action against the power thefts. In the 3rd section, we discussed the various methods for fraud. In the 4th section, we analysed the performance analysis of those methods. In the 5th section, we researched and debated the flows in the approaches discussed in sections 3 and 4. Also, we discussed the space for improvement in those approaches. In the last quarter, we concluded the research study and discussed the further work of this research study.

II. Reason Behind the Power Theft

Several reasons for electricity theft are described in the literature [26]. All those factors are categorised into two categories A) Political reasons and B) Socioeconomic reasons.

A. Political reasons

According to the World Bank survey, if the countries face political issues, political power unbalancing, civil wars, poor civil rights, the lack of accountability and lack of democratic power, there are more chances for electricity theft. These issues we can analyse in the current scenario in the Asian countries China, Pakistan, and India have many more effects sometimes due to lack of awareness, the lower standard of living, and the election season pressures. Also, sometimes the lack of proper rules and regulations to punish the fraud consumers and outdated laws become an issue, and many fraud consumers can find a loophole in the statutes. Also, according to the research study [27], [28],[29],[14], the corruption level of countries is more likely to have more numbers of fraud consumers, such as Tunisia, Pakistan, and India.

B. Socioeconomic reasons

As shown in Figure 2, the socioeconomic factors for the electricity thefts. Most the developing countries are almost suffering from these issues; as shown in the figure above, the lack of education, the did not get the proper job, and a good salary which is not good enough to pay basic expenses, and they cannot easily afford the

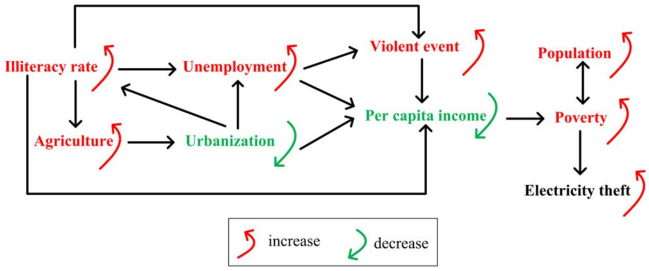

Figure 2 Correlation of various socioeconomic reasons for the power theft[10]

electricity which encourages them to steal the power from the grid[30]. As the population increases and full fill their food-related requirements, there is a rise in the farming sector, which is positive. Still, it also needs electricity to run the water pumps and much other agricultural equipment, and the timing for the power supply into the farm was not correctly scheduled[31]. Significantly less power is supplied to the agriculture as per the previous agriculture information, which makes them steal the energy from the girds.

C. Other reasons

Other than these two factors, many other factors encourage the people to steal the power from the girds. The rise in global warming and the increase in heatwaves in many world regions increase the number of electricity users (Air conditions, coolers, Fridges), which consumes reactive power and costs more than the average power consumption. Their invoice amount is on the higher side. Also, in many developing countries, this electric power distribution is still managed by the government authorities, and their lack of monitoring leads to more cases of electricity theft.

D. Government mandates to prevent the electricity theft

TABLE II. GOVERNMENT MANDATES TO PREVENT THE ELECTRICITY THEFT[10]

Countries	Laws	Punishments
UK	Energy theft law 1968	Up to five years of presentment if caught in the act.
India	The act of electricity 2003	Six months to five years of presentment with the fine of the three times of energy is stolen from the power grids.
Pakistan	Pakistan electricity pean code 2016	Up to three years of presentment and a fine of up to 10M Pakistani rupees
China	Electricity laws	Up to five times a fine of energy was stolen, and points decrement in the social scores.
Turkey	Criminal code	Presentment of one to five years
Algeria	Criminal act 350	Presentment of one to five years with the fine of 500 to 20K dinars
Nigeria	Nigerian energy commission	Fine Up to 50K – 200K Nigerian dollars

III. ELECTRIC POWER THEFT DETECTION METHODS

In the 0nd section, we discuss the various factors and the reasons for the electricity theft and the people's mindset behind the stealing the electric power. Also, it analysed how this power theft is a risk to the electric networks and the other consumers [32]. The power utilities of authorised persons validate power usage from one house to another using an energy meter [33]. Different methods have been utilised to detect power theft, such as hardware-based, state space-based, game theory-based, and data-driven [34]. All those methods are discussed in this section.

A. Hardware-based methods

Many distribution companies face this issue of electricity theft. To solve the problem, they implemented a physical hardware-based model with specific energy measurement meters with anti-tampering inbuilt functions and AMI-based meters that can transmit the dataset with the help of RFID sensors[35]. All this information is supplied through the WAN and LAN based connection. Due to availability of the affordable and fast internet, all this information is passed to the government authority or the distribution companies. All those information is manually analysed based on the electronics hardware applied in the networks [36].

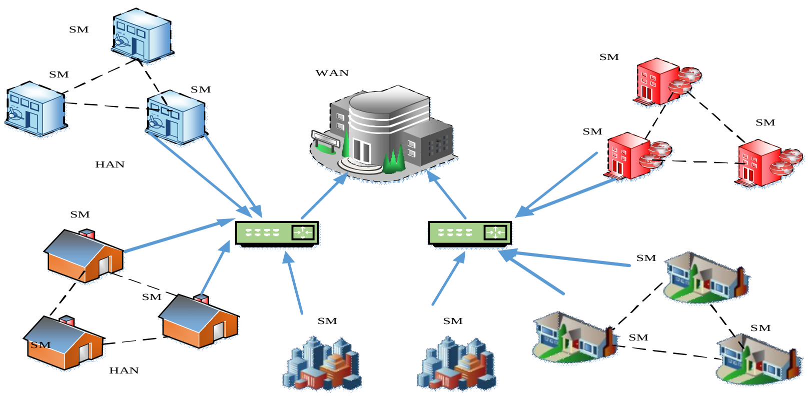

Figure 3 Simple advanced headwear and metering infrastructures

B. State space-based modelling approaches

The power systems are constantly analysed and designed from the State space-based models. These state space-based models consist of every component of the power system network and are utilised as state-space equations [37]. This control system space designs the combination of the voltage and current based features in the power system networks. For the theft detection in the electrical power grid, this approach required every component connected to the grid, which also included every element of the consumer end and based on these components, this method utilised the audit based information from the power utility company as well as the power consumed by each consumer end components and based on this audit we can able to identify the fraud consumer in the power grid [21].

C. Game theory-based approaches

This is an AI agent-based approach. In this method, the entity based agents were created in the virtual environments. For this problem of theft detection, first, the virtual environments were designed to replicate real-world situations. For example, the environment consists of power consumption rates, tariff rates, and various entities such as industrial consumer agents, agriculture consumer agents, Domestic consumer agents, and commercial consumer agents. When these agents were created, the different function of the agents was applied based on their power consumption pattern in the real world to replicate the real-world situations[38]. Once this agent was set, one more agent was created, which played the role of the power distribution company with the function of power supply as per the needs in the grids and collected the data information of the consumer power consumption. Now all the environments and agents were set. Then one small mole in the agents was created, which tried to steal the electricity from the grid by illegally connecting the load to the grid by bypassing the meter connection. This type of electric theft occurs when the distribution company and consumer power data are recorded and thoroughly analysed in the simulation environment [39]. Based on these fundaments, real-time models are created if a similar pattern is observed that the consumer keeps under observation for fraud detection and substantial evidence collection.

Using this algorithm, the underdog power theft pattern dataset was collected, which is very difficult to analyse on the real-world data due to their regular usage of the power, which might misguide the power distribution companies.

D. Data-driven approach

Power theft is detected by data-driven methods such as decision tree [40], linear regression [41], state estimation [42], supervised learning [43], deep learning [44], game theory method [33] and long-short term memory-based neural network methods [45]. Power theft is effectively detected by a classification-based framework from all these methods. The Electricity theft detection using a classification-based framework is shown in Figure 4 [46].

Machine learning-based model

The progressive metering arrangement permits the mutual distribution of data among smart meters and services. Nevertheless, the power theft of the cyber-security problem in the smart grid is a significant problem. Therefore, Sravan and Dipu Sarkar [47] developed an ensemble-based machine learning framework for power theft detection in a grid system by the user's depletion method. The ensemble machine learning method encloses extreme boosting, adaptive, light boosting, categorical enabling extra, and random forest method has been used

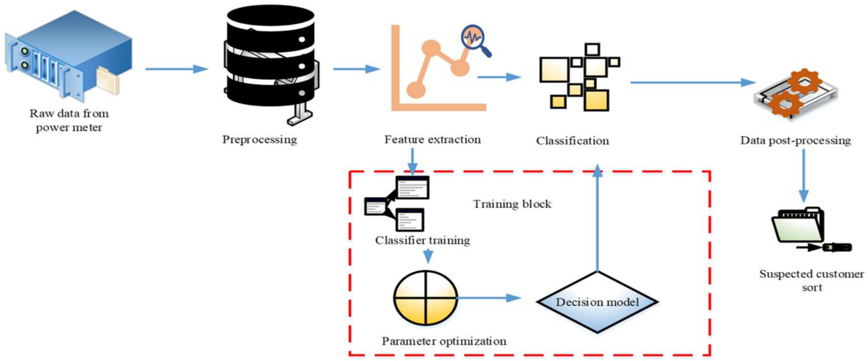

Figure 4 Electricity theft detection using the data-driven classification based approaches

to estimate the detection degrees and false positives. The information pre-processing technique enhances the detection function. The Area under Curve (AUC) of different trees and random forest method has been achieved as 0.90.

Rajiv Punmiya and Sangho Choe [48] developed an improved machine learning method named extreme gradient boosting (XGBoost) for Time-Of-Use (ToU) power theft activities. The cost of electricity varies throughout the day depending upon consumers' decisions in ToU. A few malicious users can take power and operate the detailed theft detection report. The false-positive rate off-ToU has achieved 3%, and d-ToU has 4%. Moreover, the detection rate of dynamic ToU has been obtained as 98%.

Power theft is a big problem in the power distribution segment, and its detection methods have improved in many studies. The inadequate tuning and prohibited energy meters develop many non-technical based losses. This loss can create vast financial problems and security issues in the power network. In some cases, it cannot remove the power theft in most power distribution industries, which can be detected and prevented. For this reason, Behc and vendetta [49] developed a Long-Short-Term Long Memory (LSTM) that depends on deep learning techniques for power theft detection. The schematic of LSTM in power theft recognition is illustrated in Fig.4.

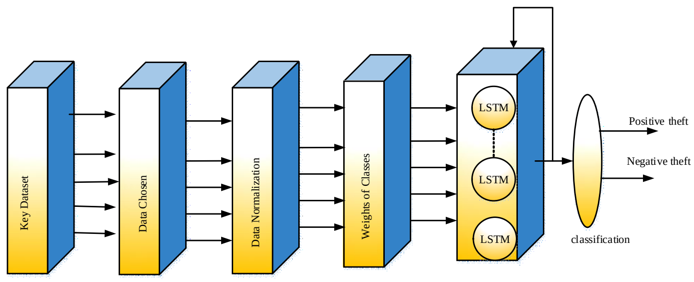

Figure 5 Schematic structure diagram of the LSTM modelsz

The reliability of the power system is regulated by proficient power theft detection. Moreover, the innovative grid development and conventional power theft detection methodologies have increased the challenges. Therefore, a new enhanced random forest (RF) and synthetic minority oversampling technique (SMOTE) is introduced by Zhengwei Qu et al. [50] for effective power theft recognition. The K-means clustering has balanced the data with SMOTE (K-SMOTE) algorithm. Then, the balanced data was trained using the RF method and effectively detected the power theft on the consumer end.

Power theft has become a great challenge for power operators and must be recognised and reduced. Power theft became widespread when advanced metering infrastructure (AMI) developed in the smart grid. For this reason, Blazakis and Georgios [51] developed a new data mining based method stated as Density-Based Spatial Clustering of Applications through Noise (DBSCAN) for the illegal energy consumption detection. The diverse electricity theft is analysed by principal component analysis (PCA) combined with the mean shift method. The throughout work outcomes demonstrate that the developed method can enhance the power system's security, reliability, and working.

Extreme collective technical and commercial losses are the main problems in electricity usage. Many innovative methodologies have been introduced in metering structures to reduce the pain in power systems. However, the inventive method does not provide proper performance in some activities. Hence, Majid Aryanezhad [52] introduced an online-based power theft detection and prevention method based on real-time situations. A new electricity pilferage prevention system (EPPS) is projected to provide proper voltage maintenance to the power system even under the illegal load connection. The projected method improves the power distribution system's reliability, revenue, flexibility, and suitability. The accuracy of the detected power theft is 99% achieved.

Supriya Jaiswal and Makarand S. Ballal [53] projected a fuzzy inference on the electricity theft prevention system (ETPS) using LabVIEW for real-time based power theft estimation. Moreover, the consumer care unit (CCU) is associated with ETPS to regulate the legal user side voltage supply. Because the power distribution segment on the utility side can be mainly affected by the power theft problem. The reliability and stability of the power supply are regulated. This method is validated under the direct tapping situation on the distribution line. The losses were reduced up to a negative 1.31% under 2235.5 Wh.

The security of the smart grid is enhanced by proficient power theft detection. However, in advanced metering infrastructure (AMI), the deep learning method plays a significant part in theft detection. Therefore, Jiangnan Li [54] investigated a proficient function of the deep learning method for electricity theft detection. The iterative and single-step assault is taken to validate the operation of the projected approach. The confrontational assailants can explosion tremendously low depletion capacities to the usefulness deprived of being noticed through the deep learning representations. Consequently, the possible protection devices compared to vicious assaults in vitality theft recognition.

J. Nagi et al. [55] developed a new Support Vector Machine (SVM) based intelligent power theft detection approach because of fraudulent power depletion. The non-technical loss caused by the power theft in the distribution segment is detected in this work. The projected ideal preselects supposed customs to be reviewed onsite for deception depending on indiscretions and irregular depletion performance. Moreover, this method delivers a data mining technique that includes feature mining as ancient consumer depletion statistics—the SVM method customs consumer load summary material to depict irregular performance connected with technical loss happenings. Furthermore, the consequence produces classification sessions utilised to choose possible deception defendants for onsite examination, depending on substantial performance that appears because of abnormalities in depletion. The Summary of machine learning-based power theft detection is illustrated in Table .

TABLE III. SUMMARY OF THE MACHINE LEARNING-BASED APPROACH FOR THE ELECTRIC FRAUD DETECTION

Author	Methods	properties	Merits	Limitation
Sravan and Dipu Sarkar [47]	Ensemble Machine learning	5000 customers	Highest AUC is obtained	Accuracy is less
Rajiv Punmiya and Sangho Choe [48]	XGBoost	1000 customers	Applicable in real-time usage	The classification problem is big
Behc and vendetta [49]	ETD-LSTM	33.979 customers	Feature extraction is high	Required real-time verification
Zhengwei Qu et al. [49]	K-SMOTE	368 users	Stronger stability	The error rate is a bit high
Blazakis and Georgios [50]	DBS	1100	The success rate is high	Performance metrics are not validated
Majid Aryanezhad[51]	EPPS	-	Improved accuracy and Complexity are low.	The computational period is high.
Supriya Jaiswal and Makarand S. Ballal [52], [53]	Fuzzy ETPS	51 consumers	Financial loss is reduced and provides simplicity	Performance metrics are failed to validate
Jiangnan Li [54]	DNN	48 power data	Improved security.	Attackers' cost is high.
J. Nagi et al. [55]	SVM	186,968 customers	Reliability	Accuracy is less

Hybrid machine learning-based approach for theft detections

In power industries, the quality of power supply, non-technical losses, and grid working safety caused by power theft are the main concerns for financial losses. For this reason, Xiangyu Kong et al. [56] projected a combination of methods termed Decision Tree Incorporated with K-Nearest Neighbor Along With Support Vector Machine (DT-KSVM) for power theft identification. Initially, the kernel fuzzy-based C-means (KFCM) algorithm is applied for the feature selection method in consumers' standard power depletion feature curve. Then the AMI was utilised to resolve the data stolen issues. The stealing data has been executed by The One-Dimensional Based Wasserstein Generative Adversarial Networks (1D-WGAN). Consequently, DT-KSVM is utilised to accomplish subordinate recognition and classify apprehensive consumers. The representation of DT-KSVM is illustrated in Figure 6.

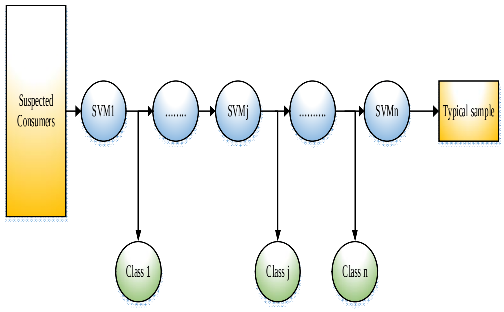

Figure 6 Decision tree base hybrid support vector Machin learning algorithm for the fraud detections

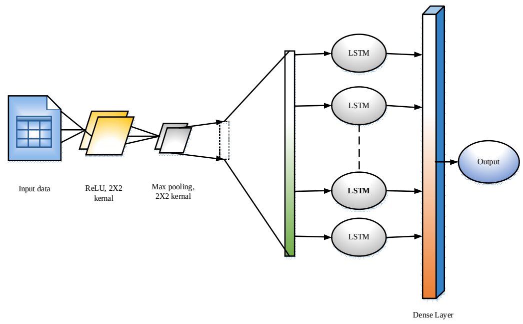

Figure 7 Hybrid CNN+LSTM model construction

Zhong Tao et al. [57] introduced a novel Electricity Theft Detection based on Deep Bidirectional Combined Recurrent Neural Network (ETD-DBRNN) method for power theft detection. Power theft creates a significant problem for financial and community improvement. Generally, the power depletion data method depends on power theft detection can assist in resolving this issue. However, conventional techniques have inappropriate accuracy for theft estimation, and they can easily be affected by the outer impact of characteristics. For this reason, only the ETD-DBRNN method is developed for the inner and outer correlation using the power depletion data and other characteristic features.

The AMI is combined with the novel method for the power theft detection introduced by Matheus et al. [58] in the distribution system. The power theft evidence is taken by estimating a three-phase based state estimator depending on phasor measurement components in the transformer unit. Consequently, the stealing power identification by the user is the other stage. The Self-Organizing Map (SOM) method has trained the user power consumption data group. The new Multilayer Perceptron based Artificial Neural Network (MP-ANN) is executed for the classification of power theft or not. The execution of this work is validated under the IEEE 70 bus system, and 5000 fake users of accurate data are taken. Moreover, 93% of fault detection value has also been achieved significantly less false positive value is reached. The main aim of this power theft identification is to reduce the measurement components in each transformer.

Development has been fast-moving up communal and financial changes in urban societies. Nevertheless, urban regulation and secrecy became a significant task in urbanisation. Hence, a risk forecast method is necessary to inhibit and prevent crime in urban groups. To overcome such issues, a Long Short-Term Memory Network (LSTM), in addition to Spatial-Temporal Graph Convolutional Network (ST-GCN), is projected by Xinge Han et al. [59] for high-risk power theft detection in an automatic way.

Smart grids trust Info and Infrastructures Knowledge and intelligent meters to the mechanism and accomplish frequent system criticisms. Nevertheless, using these structures' variety of intelligent grids is susceptible to fake intimidation, particularly power theft. Hence, the power theft detection method plays an essential part in power system non-technical loss problems. Hossein proposes an Ensemble-based Deep Convolutional Neural Network (EDCNN) method [60] for power theft prediction in smart grids. Primarily, the bagging method is provided to the system for unstructured data, and sequentially EDCNN is used. The performance metrics are estimated for the validation of this work.

In a power system, the power loss is estimated based on the condition of technical failures and non-technical losses. Nevertheless, the non-technical based loss highly impacts the grid over the technical problem due to billing errors, faulty meters, and power theft. Thus, power theft has caused more financial issues in utility industries in modern power systems. Traditionally, power theft detection has high challenges due to the overfitting problem, unstructured data, and massive aspect of data handling. An LSTM method is introduced with the bat combined random under-sampling boosting (RUS Boost) method for abnormal power theft detection by Muhammad Adil et al. [61] to overcome this limitation. The feature extraction has been done by the LSTM method. The RUS Boost method is utilised for the classification of false detection. The receiver operating characteristics (ROC), precision, F1-score and recall based performance evaluation are examined.

The literature [62] developed a new power theft detection method. Thus, the State Grid Corporation of China (SGCC) based dataset is taken to validate the developed method under the cases of typical theft conditions. This dataset is enclosed with numerous misplaced and mistaken rates. Also, the empirical mode decomposition method has been utilised to pre-process the data and feature selection. Then a new K-nearest neighbours (KNN) method was applied to the system to improve the accuracy in a rapid and straightforward process. The power theft detection method has attained 91.0% of accuracy.

Among all non-technical based losses, power theft became a highly challenging and severe problem. Power theft causes some problematic issues such as quality of power supply, generation load raises users' power bill problems and affect overall financial situations. The data analysis method has been utilised to diminish the loss in the innovative grid operation. The smart grid structure creates a large quantity of data that encloses the energy depletion of solitary consumers. Hence, Md. Nazmul Hasan et al. [63] developed an LSTM based convolutional neural network (CNN) of integration for power theft identification. The structure of the CNN-LSTM model is shown in Figure 7 The classification and feature extraction has been done using CNN. The missing data in the dataset for power theft detection is pre-processed by this novel method.

Konstantinos V. Blazakis et al. [64] developed a new Adaptive Neuro-Fuzzy Inference System (ANFIS) method for power theft detection in smart grids. The developed method provides high positive value in different belongings of deceitful actions invented from illegal power convention.

TABLE IV. SUMMARY OF THE KINDS OF LITERATURE RELATED TO THE HYBRID MACHINE LEARNING ALGORITHMS

Author	Methods	properties	Merits	Limitation
Xiangyu Kong et al.	DT-KSVM	6400 pieces	Under the abnormal data also, the detection accuracy is high	However, the accuracy of the conventional methods is high then this method
Zhongtao et al. [56]	ETD-DBRNN	5000 Irish homes	A high recall index was achieved	Further improvement is required
Matheus et al. [59]	MP-ANN	5000 consumers	the secrecy of consumers is taken	Expense is increased
Xing Han et al. [38]	LSTM and ST-GCN	77 communities	More accurate over other methods	Certain training complexity is present
Hossein [59]	EDCNN	42372 users	The false-positive rate is low, and accuracy is more	The inside attack detection is not well developed.
Muhammad Adil et al. [61]	Bat- RUS Boost	5000 users	Reliability is improved	Accuracy is low
Sumair Aziz et al.[62]	KNN	1,035 days	Cost-efficient and rapid process	Accuracy is less than other methods

IV. PERFORMANCE METRICS

The performance metrics are validated for various power theft detection methods in accuracy, precision, recall, F1-score, computational time, RoC and AUC. The machine learning and hybrid form of machine learning in power theft detection are validated in this investigation. The machine learning method provides high accuracy and diminishes the computational period. However, the advanced hybrid machine learning approach provides a significant outcome under abnormal data.

A. Models' performance accuracy

The accuracy is defined as the exact theft detection compared with the diverse conventional methods illustrated. The accuracy of the diverse method has been validated from that the Ensemble Machine learning [65] has 82.5% of accuracy, ETD-LSTM [48] has 93% of accuracy, K-SMOTE [49] has 94.53% of accuracy, Fuzzy ETPS [52] has 98.2% of accuracy, DNN [53] has 97.7% of accuracy, SVM [54] has 72.60% of accuracy, DT-KSVM [56] has 95.6% of accuracy, ETD-DBRNN [57] has 97.44% of accuracy, EDCNN [57] has 98.1% of accuracy, Bat-RUS Boost [62] has 87.9% of accuracy, and CNN-LSTM [63] has 89% of accuracy. However, the typical Fuzzy ETPS [52] based machine learning methods achieved higher accuracy than other methods.

B. Precision of model's predictions

The performance metrics comparison of precision rate is defined as the ratio of consumers that are appropriately detected by way of typical each user identified as usual. The precision value obtained from various power theft detection methods is validated, shown in Figure 9. The comparison obtained by Ensemble Machine learning [65] has acquired 99% of precision, ETD-LSTM [48] has got 92% of accuracy, ETD-DBRNN [57] has received

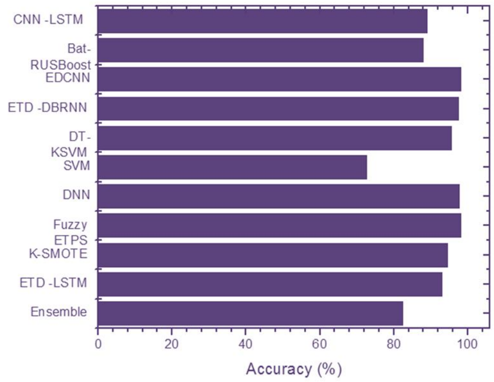

Figure 8 Comparison of various machine learning methodologies in Accuracy

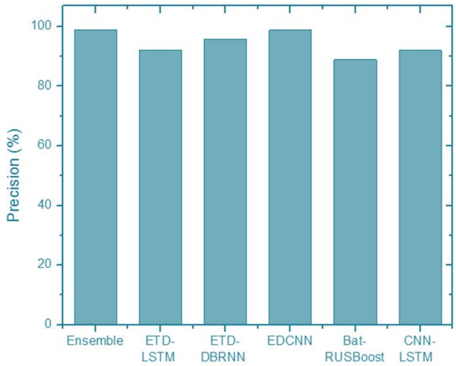

Figure 9 Models precision compression

95.70% of precision, EDCNN [60] has acquired 98.8% of precision, Bat-RUS Boost [61] has obtained 88.9% of accuracy, and CNN-LSTM [63] has received 92% of precision.

C. Recall based prediction model's performance analysis

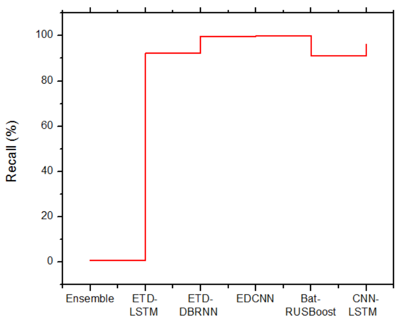

Figure 10 Recall based model prediction performance analysis

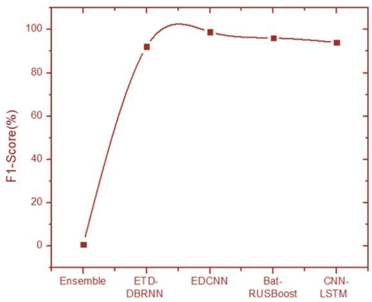

Figure 11 F1 score-based models prediction performance

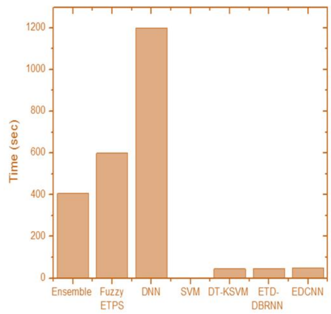

Figure 12 Overall cooperation of all machine learning models for the fraud detection

Consequently, the recall states that the ratio of appropriately identified optimistic consumers per the amount of each consumer. The recall value obtained from various power theft detection methods is validated, shown in Figure 10. The comparison obtained Ensemble Machine learning [65] has received 75% of recall, ETD-LSTM [48] has obtained 92.22% of memory, ETD-DBRNN [57] has acquired 99.74% of remembrance, EDCNN [60] has received 99.90% of recall, Bat-RUS Boost [61] has obtained 91.09% of memory, and CNN-LSTM [63] has acquired 96% of remembrance.

D. F1 Score based performance measurements

The F1-score value obtained from several power theft detection methods is validated, shown in Fig.10. The comparison obtained by Ensemble Machine learning [65] has received 75% of the F1 score, ETD-DBRNN [57] has acquired 92.09% of the F1 score, EDCNN [39] has obtained 98.9% of the F1 score, Bat-RUS Boost [61] has received 96.1% of F1-score, and CNN-LSTM [63] has acquired 94% of F1-score

E. Overall model comparisons

The computational time obtained from various power theft detection methods is validated, shown in Figure 12. The comparison obtained Ensemble Machine learning [65] has obtained 406 sec, Fuzzy ETPS [52] has obtained 600sec, DNN [53] has obtained 1200sec, SVM [54] has obtained 2.3 sec, DT-KSVM [56] has received 45.324sec, ETD-DBRNN [57] has got 48sec, and EDCNN [60] has got 50sec. The SVM method in power theft detection has significantly less time than the other methods.

The overall Performance metrics comparison with diverse conventional methods is detailed in Table . The discussion in Table described the accuracy, precision, recall and F1-score value of various machine learning and hybrid-based methods in power theft detection. Moreover, the different computational time, RoC, and AUC are examined in diverse ways. The performance metrics of individual machine learning, hybrid machine learning model, and optimisation combination are studied.

Table V. Overall Performance Compression with Different Classification Metrics

Method	Accuracy	Precision	Recall	F1-score	Time	RoC	AUC
Ensemble Machine learning [65]	82.5	99	0.75	0.75	406 s	0.9	0.90
ETD-LSTM [48]	93	92	92.22	NA*	- NA	- NA	- NA
K-SMOTE [49]	94.53	- NA	- NA	- NA	- NA	0.91	0.951
Fuzzy ETPS [52]	98.2	- NA	- NA	- NA	600sec	- NA	- NA
DNN [53]	97.7	- NA	70	- NA	1200 sec	- NA	- NA
SVM [54]	72.60	- NA	- NA	- NA	2.3 sec	- NA	- NA
DT-KSVM [56]	95.6	- NA	- NA	- NA	45.324sec	- NA	0.85
ETD-DBRNN [57]	97.44	95.70	99.74	92.09	48sec	- NA	- NA
EDCNN [60]	98.1	98.8	99.90	98.9	50sec	- NA	0.993
Bat-RUS Boost [61]	87.9	88.9	91.09	96.1	- NA	0.87	- NA
CNN-LSTM [63]	89	92	96	94	- NA	- NA	- NA

*NA – No data founded

V. Discussion on Method Selections

Based on various methodologies, the primary method for fraud detection is to deploy the AMI based meter system and continually analyse the consumption information. One of the critical issues is the initial cost of headwear system deployment and the many workforces taken for examining the dataset continuously coming from consumer ends—the unreliability of the hardware system during challenging weather conditions. The overall maintenance cost of the hardware system is more. For this approach, if any data science approach processes the collected data, that would be better for the analysis.

The classic state-space based methods for fraud detection also provided great simulation accuracy. However, implementing this approach is very challenging because to identify the fraud consumer, this method requires detailed information about the power consumers about the equipment they utilised and based on the elements and their operation time, one state-space block is created, and this same way, a new state-space block is is making. Also, this information is too large to handle, and continuously combining data information from the consumer end, this method is quite bookish to implement.

The advantages and drawbacks of numerous machine learning approaches for power theft detection were examined in this review article. Additionally, to suggest a new technique based on this review, the legal restriction of all forecast models is studied. The corporate advantages and drawbacks of machine learning methods for power theft detection are detailed in Table VIVI.

TABLE VI. ADVANTAGES AND DISADVANTAGES OF MACHINE LEARNING MODELS

Methods	Advantages	Drawback
Machine learning	• The turns of events and arrangements are effectively perceived. • A large amount and high dimensional information can deal with	• Results may fluctuate. • It requires more opportunity to contemplate and make the capacity with the exact outcome.
Hybrid machine learning	• Upgraded radically • Under the unstructured data, likewise, the best results are accomplished. • Can settle the advancement issues • Addressing the quantitative issues • Best results can acquire.	• For preparing, a gigantic measure of information is needed • More time is taken to prepare the information • The element choice depends on the reliant capacity. • The assessment of execution boundary is almost sluggish.

VI. Conclusion

This research work is a review work based on the electricity theft detection and analysed the various recent research work and studies what sort of methodologies they apply to detect the fraud consumer from the large gird and what type of consideration we needed to take while creating the models. Before that, we discussed how much this electricity theft costs to the government authorities and many distribution companies. Based on the authenticated data information, it is founded that this is a severe issue. It can cause severe damage to the power grid lines, the other available consumers, the girds, and the power generation units. After this discussion, we study what type of mandates are passed by the various governments to prevent electricity theft. After discussing the electric robbery and the government mandate, different recent methodologies and their research work are thoroughly studied and discussed. Their research work also tries to do a little bit of critical analysis in their research work in the discussion sections. We suggest utilising supervised and unsupervised machine learning-based approaches based on this research work-study. For the imbalances, classification classes SMOTE, Adasyn based system can be used. The class weightage-based system can provide accurate results without adding synthetic data to the dataset.

REFERENCES

[1] T. Austin, E. Larson, and D. Ernst, "SimpleScalar: an infrastructure for computer system modeling," *Computer (Long Beach Calif)*, vol. 35, no. 2, pp. 59–67, 2002, doi: 10.1109/2.982917.

[2] H. Nagayama, "Electric power sector reform liberalization models and electric power prices in developing countries," *Energy Economics*, vol. 31, no. 3, pp. 463–472, May 2009, doi: 10.1016/j.eneco.2008.12.004.

[3] R. Amarnath, N. Kalaivani, and V. Priyanka, "Prevention of power blackout and power theft using IED," in *2013 IEEE Global Humanitarian Technology Conference (GHTC)*, Oct. 2013, pp. 82–86. doi: 10.1109/GHTC.2013.6713659.

[4] J. Sijm, K. Neuhoff, and Y. Chen, "CO_2 cost pass-through and windfall profits in the power sector," *Climate Policy*, vol. 6, no. 1, pp. 49–72, Jan. 2006, doi: 10.1080/14693062.2006.9685588.

[5] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, Feb. 2011, doi: 10.1016/j.enpol.2010.11.037.

[6] Y. P. Siwakoti and F. Blaabjerg, "Common-Ground-Type Transformerless Inverters for Single-Phase Solar Photovoltaic Systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2100–2111, Mar. 2018, doi: 10.1109/TIE.2017.2740821.

[7] M. Wolsink, "The research agenda on social acceptance of distributed generation in smart grids: Renewable as common pool resources," *Renewable and Sustainable Energy Reviews*, vol. 16, no. 1, pp. 822–835, Jan. 2012, doi: 10.1016/j.rser.2011.09.006.

[8] M. ASIF and T. MUNEER, "Energy supply, its demand and security issues for developed and emerging economies," *Renewable and Sustainable Energy Reviews*, vol. 11, no. 7, pp. 1388–1413, Sep. 2007, doi: 10.1016/j.rser.2005.12.004.

[9] P. G. Kate and J. R. Rana, "'ZIGBEE based monitoring theft detection and automatic electricity meter reading,'" in *2015 International Conference on Energy Systems and Applications*, Oct. 2015, pp. 258–262. doi: 10.1109/ICESA.2015.7503351.

[10] X. Xia, Y. Xiao, W. Liang, and J. Cui, "Detection Methods in Smart Meters for Electricity Thefts: A Survey," *Proceedings of the IEEE*, vol. 110, no. 2, pp. 273–319, Feb. 2022, doi: 10.1109/JPROC.2021.3139754.

[11] P. R., "World loses $89.3 billion to electricity theft annually, $58.7 billion in emerging markets," 2014.

[12] "Analysis: Electricity Theft in South Africa. Metering & Smart Energy International," 2017.

[13] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in *2011 IEEE/PES Power Systems Conference and Exposition*, Mar. 2011, pp. 1–8. doi: 10.1109/PSCE.2011.5772466.

[14] Sudhir Kumar Katiyar, "Political Economy of Electricity Theft in Rural Areas: A Case Study from Rajasthan," *JSTOR*, vol. 40, no. 07, pp. 644–648, Feb. 2005.

[15] V. Gaur and E. Gupta, "The determinants of electricity theft: An empirical analysis of Indian states," *Energy Policy*, vol. 93, pp. 127–136, Jun. 2016, doi: 10.1016/j.enpol.2016.02.048.

[16] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering Infrastructure," *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 473–484, Dec. 2014, doi: 10.1016/j.ijepes.2014.06.025.

[17] R. Burgess, M. Greenstone, N. Ryan, and A. Sudarshan, "The Consequences of Treating Electricity as a Right," *Journal of Economic Perspectives*, vol. 34, no. 1, pp. 145–169, Feb. 2020, doi: 10.1257/jep.34.1.145.

[18] J. C. Y. Wong, B. Blankenship, J. Urpelainen, K. Ganesan, K. Bharadwaj, and K. Balani, "Perceptions and acceptability of electricity theft: Towards better public service provision," *World Development*, vol. 140, p. 105301, Apr. 2021, doi: 10.1016/j.worlddev.2020.105301.

[19] R. Chakraborty, A. Samanta, K. M. Agrawal, and A. Dutta, "Towards smarter grid: Policy and its impact assessment through a case study," *Sustainable Energy, Grids and Networks*, vol. 26, p. 100436, Jun. 2021, doi: 10.1016/j.segan.2021.100436.

[20] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105–120, Apr. 2014, doi: 10.1109/TST.2014.6787363.

[21] J. B. Leite and J. R. S. Mantovani, "Detecting and Locating Non-Technical Losses in Modern Distribution Networks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1023–1032, Mar. 2018, doi: 10.1109/TSG.2016.2574714.

[22] P. Chandel, T. Thakur, B. A. Sawle, and R. Sharma, "Power theft: Major cause of non technical losses in Indian distribution sector," in *2016 IEEE 7th Power India International Conference (PIICON)*, Nov. 2016, pp. 1–6. doi: 10.1109/POWERI.2016.8077253.

[23] F. B. Lewis, "Costly 'Throw-Ups': Electricity Theft and Power Disruptions," *The Electricity Journal*, vol. 28, no. 7, pp. 118–135, Aug. 2015, doi: 10.1016/j.tej.2015.07.009.
[24] G. L. Prashanthi and K. v Prasad, "Wireless power meter monitoring with power theft detection and intimation system using GSM and Zigbee networks," Ver. I. [Online]. Available: www.iosrjournals.org
[25] R. Razavi and M. Fleury, "Socio-economic predictors of electricity theft in developing countries: An Indian case study," *Energy for Sustainable Development*, vol. 49, pp. 1–10, Apr. 2019, doi: 10.1016/j.esd.2018.12.006.
[26] D. N. Nikovski *et al.*, "Smart Meter Data Analysis for Power Theft Detection," 2013, pp. 379–389. doi: 10.1007/978-3-642-39712-7_29.
[27] T. Sharma, K. K. Pandey, D. K. Punia, and J. Rao, "Of pilferers and poachers: Combating electricity theft in India," *Energy Research & Social Science*, vol. 11, pp. 40–52, Jan. 2016, doi: 10.1016/j.erss.2015.08.006.
[28] F. Jamil and E. Ahmad, "An Empirical Study of Electricity Theft from Electricity Distribution Companies in Pakistan," 2014.
[29] M. Golden and B. Min, "Theft and Loss of Electricity in an Indian State," 2012.
[30] W. E. Becker and D. R. Lewis, "PREVIEW OF HIGHER EDUCATION AND ECONOMIC GROWTH."
[31] S. Mariam, "The Effects of Unemployment on Crime Rates in the U.S," 2007.
[32] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016, doi: 10.1109/TSG.2015.2425222.
[33] K. Zheng, Q. Chen, Y. Wang, C. Kang, and Q. Xia, "A Novel Combined Data-Driven Approach for Electricity Theft Detection," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1809–1819, Mar. 2019, doi: 10.1109/TII.2018.2873814.
[34] F. Xiao and Q. Ai, "Electricity theft detection in smart grid using random matrix theory," *IET Generation, Transmission and Distribution*, vol. 12, no. 2, pp. 371–378, Jan. 2018, doi: 10.1049/iet-gtd.2017.0898.
[35] M. F. McGranaghan, S. Santoso, R. C. Dugan, and H. W. Beaty, *Electrical Power Systems Quality, Third Edition*. <country>US</country>: McGraw-Hill Professional, 2012. doi: 10.1036/9780071761567.
[36] K. Dineshkumar, P. Ramanathan, and S. Ramasamy, "Development of ARM processor based electricity theft control system using GSM network," in *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, Mar. 2015, pp. 1–6. doi: 10.1109/ICCPCT.2015.7159401.
[37] S. Salinas, M. Li, and P. Li, "Privacy-Preserving Energy Theft Detection in Smart Grids: A P2P Computing Approach," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 257–267, Sep. 2013, doi: 10.1109/JSAC.2013.SUP.0513023.
[38] A. A. Cardenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct. 2012, pp. 1830–1837. doi: 10.1109/Allerton.2012.6483444.
[39] L. Wei, A. Sundararajan, A. I. Sarwat, S. Biswas, and E. Ibrahim, "A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game," in *2017 Resilience Week (RWS)*, Sep. 2017, pp. 5–11. doi: 10.1109/RWEEK.2017.8088640.
[40] 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, Jun. 2016, doi: 10.1109/TII.2016.2543145.
[41] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," *International Journal of Electrical Power & Energy Systems*, vol. 91, pp. 230–240, Oct. 2017, doi: 10.1016/j.ijepes.2017.04.005.
[42] S.-C. Huang, Y.-L. Lo, and C.-N. Lu, "Non-Technical Loss Detection Using State Estimation and Analysis of Variance," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2959–2966, Aug. 2013, doi: 10.1109/TPWRS.2012.2224891.
[43] Z. A. Khan, M. Adil, N. Javaid, M. N. Saqib, M. Shafiq, and J.-G. Choi, "Electricity Theft Detection Using Supervised Learning Techniques on Smart Meter Data," *Sustainability*, vol. 12, no. 19, p. 8023, Sep. 2020, doi: 10.3390/su12198023.
[44] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018, doi: 10.1109/TII.2017.2785963.
[45] N. Somu, G. R. M R, and K. Ramamritham, "A hybrid model for building energy consumption forecasting using long short term memory networks," *Applied Energy*, vol. 261, p. 114131, Mar. 2020, doi: 10.1016/j.apenergy.2019.114131.
[46] R. Razavi, A. Gharipour, M. Fleury, and I. J. Akpan, "A practical feature-engineering framework for electricity theft detection in smart grids," *Applied Energy*, vol. 238, pp. 481–494, Mar. 2019, doi: 10.1016/j.apenergy.2019.01.076.
[47] S. K. Gunturi and D. Sarkar, "Ensemble machine learning models for the detection of energy theft," *Electric Power Systems Research*, vol. 192, p. 106904, Mar. 2021, doi: 10.1016/j.epsr.2020.106904.
[48] R. Punmiya and S. Choe, "ToU Pricing-Based Dynamic Electricity Theft Detection in Smart Grid Using Gradient Boosting Classifier," *Applied Sciences*, vol. 11, no. 1, p. 401, Jan. 2021, doi: 10.3390/app11010401.
[49] B. Kocaman and V. Tümen, "Detection of electricity theft using data processing and LSTM method in distribution systems," *Sādhanā*, vol. 45, no. 1, p. 286, Dec. 2020, doi: 10.1007/s12046-020-01512-0.

[50] Z. Qu, H. Li, Y. Wang, J. Zhang, A. Abu-Siada, and Y. Yao, “Detection of Electricity Theft Behavior Based on Improved Synthetic Minority Oversampling Technique and Random Forest Classifier,” *Energies (Basel)*, vol. 13, no. 8, p. 2039, Apr. 2020, doi: 10.3390/en13082039.

[51] D. Odoom, “A METHODOLOGY IN UTILIZING MACHINE LEARNING ALGORITHM FOR ELECTRICITY THEFT DETECTION IN GHANA.” [Online]. Available: https://ssrn.com/abstract=3659614

[52] M. Aryanezhad, “A novel approach to detection and prevention of electricity pilferage over power distribution network,” *International Journal of Electrical Power & Energy Systems*, vol. 111, pp. 191–200, Oct. 2019, doi: 10.1016/j.ijepes.2019.04.005.

[53] S. Jaiswal and M. S. Ballal, “Fuzzy Inference Based Electricity Theft Prevention System to Restrict Direct Tapping Over Distribution Line,” *Journal of Electrical Engineering & Technology*, vol. 15, no. 3, pp. 1095–1106, May 2020, doi: 10.1007/s42835-020-00408-7.

[54] J. Li, Y. Yang, and J. S. Sun, “Exploiting Vulnerabilities of Deep Learning-based Energy Theft Detection in AMI through Adversarial Attacks,” Oct. 2020, [Online]. Available: http://arxiv.org/abs/2010.09212

[55] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and A. M. Mohammad, “Detection of abnormalities and electricity theft using genetic Support Vector Machines,” in *TENCON 2008 - 2008 IEEE Region 10 Conference*, Nov. 2008, pp. 1–6. doi: 10.1109/TENCON.2008.4766403.

[56] X. Kong, X. Zhao, C. Liu, Q. Li, D. Dong, and Y. Li, “Electricity theft detection in low-voltage stations based on similarity measure and DT-KSVM,” *International Journal of Electrical Power & Energy Systems*, vol. 125, p. 106544, Feb. 2021, doi: 10.1016/j.ijepes.2020.106544.

[57] Z. Chen, D. Meng, Y. Zhang, T. Xin, and D. Xiao, “Electricity Theft Detection Using Deep Bidirectional Recurrent Neural Network,” in *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, Feb. 2020, pp. 401–406. doi: 10.23919/ICACT48636.2020.9061565.

[58] M. A. de Souza, J. L. R. Pereira, G. de O. Alves, B. C. de Oliveira, I. D. Melo, and P. A. N. Garcia, “Detection and identification of energy theft in advanced metering infrastructures,” *Electric Power Systems Research*, vol. 182, p. 106258, May 2020, doi: 10.1016/j.epsr.2020.106258.

[59] X. Han, X. Hu, H. Wu, B. Shen, and J. Wu, “Risk Prediction of Theft Crimes in Urban Communities: An Integrated Model of LSTM and ST-GCN,” *IEEE Access*, vol. 8, pp. 217222–217230, 2020, doi: 10.1109/ACCESS.2020.3041924.

[60] H. M. Rouzbahani, H. Karimipour, and L. Lei, “An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids,” in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2020, pp. 3637–3642. doi: 10.1109/SMC42975.2020.9282837.

[61] M. Adil, N. Javaid, U. Qasim, I. Ullah, M. Shafiq, and J.-G. Choi, “LSTM and Bat-Based RUSBoost Approach for Electricity Theft Detection,” *Applied Sciences*, vol. 10, no. 12, p. 4378, Jun. 2020, doi: 10.3390/app10124378.

[62] S. Aziz, S. Z. Hassan Naqvi, M. U. Khan, and T. Aslam, “Electricity Theft Detection using Empirical Mode Decomposition and K-Nearest Neighbors,” in *2020 International Conference on Emerging Trends in Smart Technologies (ICETST)*, Mar. 2020, pp. 1–5. doi: 10.1109/ICETST49965.2020.9080727.

[63] Md. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. M. Islam, and J.-M. Kim, “Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach,” *Energies (Basel)*, vol. 12, no. 17, p. 3310, Aug. 2019, doi: 10.3390/en12173310.

[64] K. v. Blazakis, T. N. Kapetanakis, and G. S. Stavrakakis, “Effective Electricity Theft Detection in Power Distribution Grids Using an Adaptive Neuro Fuzzy Inference System,” *Energies (Basel)*, vol. 13, no. 12, p. 3110, Jun. 2020, doi: 10.3390/en13123110.

[65] A. V. Christopher, G. Swaminathan, M. Subramanian, and P. Thangaraj, “Distribution line monitoring system for the detection of power theft using power line communication,” in *2014 IEEE Conference on Energy Conversion (CENCON)*, Oct. 2014, pp. 55–60. doi: 10.1109/CENCON.2014.6967476.