SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379 / https://doi.org/10.14445/23488379/IJEEE-V10I2P104

Volume 10 Issue 2, 35-43, February 2023

Original Article

CNN with BI-LSTM Electricity Theft Detection based on Modified Cheetah Optimization Algorithm in Deep Learning

G. P. Dimf[1], P. Kumar[2], K. Paul Joshua[3]

[1, 2]*Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India.*
[3]*St. Peter's College of Engineering and Technology, Chennai,Tamil Nadu, India,*

[1]*Corresponding Author: dimfgp02@gmail.com*

Received: 05 January 2023 Revised: 05 February 2023 Accepted: 15 February 2023 Published: 28 February 2023

Abstract *- The theft of electricity is a serious problem that all energy distribution businesses face, and it is only becoming worse. Thus, there has been an upsurge in recent years in research into techniques for identifying electricity theft. During production, incorrect and illegal energy metre calibrations could cause losses in addition to technical ones. In this paper, a bi-LSTM and convolutional neural network (CNN) are combined to propose a system for detecting electricity theft. To identify the actual daily electricity use statistics for the dataset, a Long Short-Term Memory (LSTM) based deep learning algorithm has been developed. Data classification, feature extraction, and pre-processing are a few of the techniques that have been developed. In the pre-processing stage, we prepare the data for the training model using a data pre-processing technique before removing unnecessary information. In order to enhance performance, synthetic data is also produced during the pre-processing stage. The Modified Cheetah Optimization Technique (MCHOA)-based new feature selection approach is used to choose the appropriate features for a base classifier during the feature extraction phase of the model's analysis of the voltage, current, and electric energy collected. In the classification stage, the extracted data are classified using the suggested CNN with Bi-LSTM after the feature extraction stage is completed. Whether a customer steals electricity or not, the results obtained when some techniques are combined with CNN and Bi-LSTM attain high-quality values comparable to those obtained by other methods.*

Keywords *- CNN with Bi-LSTM, Cheetah optimization technique, Deep learning, Electricity theft detection.*

1. Introduction

A major issue for the Smart Grid right now is electricity theft. The high cost of acquiring energy and the limited supply of energy sources are issues that require attention. To advance economically and socially, a nation must be energy efficient. It is, therefore, necessary to develop a model to identify electricity theft. Finding unexpected usage or activity is the main objective of Singapore's Electricity Theft Detection (ETD). By examining usage trends and looking for anomalies, it is possible to identify electricity theft. SG has emerged as a crucial tool for energy use monitoring. Computers are utilised to monitor and manage energy usage in the SG power system substructure. Additionally, it has a highly sophisticated monitoring system that keeps track of a connected consumer's usage patterns. SG offers utilities and customers the ability to monitor.

Additionally, it provides control and energy usage prediction, both of which aid in meeting user needs. The primary goal of SG is to deliver consistent energy supplies with a minimum amount of energy loss. The loss of electricity is currently the main issue impacting both conventional power networks and SGs. According to statistics, transmission and distribution losses in electricity are rising, and these losses vary by country.

Electrical power is stolen from power grids, which is considered a criminal act. This nefarious behaviour can be carried out by hacking, manipulating, or passing the power metre. Due to the capacity to access readings from smart metres and information on power use from smart grids, data-driven approaches to detecting electricity theft have recently attracted a lot of attention because they can lead to anomalous electricity consumption patterns. Next, we show how data on energy thieves' irregular electricity use may be able to be detected by machine learning algorithms. Non-technical and Technical loss (TL) loss are the two basic classifications for electricity loss (NTL). Transformer loss

(TL) is a phenomenon that develops during the transmission of energy and as a result of the joules influences on power lines. Due to the complexities of the TL calculation, it is challenging to identify a location of loss and estimate the amount of energy lost. Although TL cannot be entirely avoided, it can be minimised by using a variety of system-wide modification techniques.

These are some main contributions of this paper, like Convolutional Neural Network (CNN) and Bi-LSTM based system for detecting electricity theft. Use a pre-processing data algorithm to first prepare the data for training the model and then delete any unnecessary data. The model then analyses the voltage, current, and electric energy gathered using a novel feature selection technique based on Cheetah Optimization Technique after the feature extraction phase (CHOA). After the feature extraction stage is finished, the extracted data are then classified using the suggested CNN with Bi-LSTM. Finally, it demonstrates how to determine whether or not a consumer steals electricity.

The following sections are the remaining text of the essay. A summary of the relevant ETD work is provided in Section 2. Section 3 presents a model of the suggested CNN with Bi-LSSTM, Modified Cheetah Optimisation method. Section 4 discussion covers the simulations that were run for the proposed work. The paper is enveloped, and future work is presented in Section 5.

2. Related Work

A multi-model fusion ensemble learning strategy based on a stacking structure may identify the telltale symptoms of electricity theft. This study uses the PCA method to minimise the dimension of the user time series statistical feature indicators from the retrieved dataset. A stacking structure identification algorithm serves as the foundation for this tactic. [1] In the stacking structure's base model layer, the classifier LG + LSTM + KNN has a rapid model training time and a moderately high comprehensive evaluation value (0.9867). [2] A 2-dimensional matrix is produced from the quarterly data on planned power use as sequential input to ConvLSTM. CNN are more effective in learning data features on different quarters, months, weeks, and days when combined with long short-term memories (LSTM) [22]. An innovative end-to-end solution built on DL was created to address these challenges with electricity theft detection. A Transformer network-based model that separates out global information and determines the relative weights of attributes for customer classification. The findings demonstrate that, in the evaluation of current state-of-the-art detectors, our technique recovers features more effectively, leading to greater lower true positive rates (TPR) and false positive rates (FPR) [4] Model for detecting electricity theft based on an AMI-based stacking integrated structure. This detection model offers power grid companies a useful foundation for comparison in identifying unusual power consumption patterns, spotting users who steal electricity, increasing the success rate of on-site detection, lowering enterprise operating costs, and ensuring reliable and secure management of the power grid. [22] A defused decision boundary that causes misclassification problems because cross-pairs are present is being looked into. Due to the nature of the defused data samples, cross-pairs continue to contain cumulative attributes from both classes and mislead the classifier. [6] An integrated hybrid model composed of bi-directional gated recurrent units and bi-directional LSTM efficiently classifies consumers. The suggested model is evaluated through simulations utilising a number of performance criteria, such as recall, reliability, the area under the curve, and high accuracy.

Random undersampling, random oversampling, cost-sensitive learning and K-medoids-based under damping are some of the methods employed when a Convolutional Neural Network (CNN) is applied to the problem of detecting electricity theft. [5, 7, 9, 21, 23] Technique for Synthetic Minority Oversampling and Cluster-based Oversampling. [8] Suspect users' features are assessed using the LSTM neural network algorithm, which is also used to identify users who initially display anomalous behaviours. [24] Analysing the current, voltage and electric energy data gathered by the apparatus used to collect it enables the detection of anomalous behaviours in addition to electricity theft. [10] Analyse the techniques used by the smart grid community to identify the vulnerabilities caused by electricity theft. Data-driven models may not be as useful as they could be when fictitious measurements deviate only slightly from ingrained normal usage patterns, as we have found. Experimental results show that the new attack can be successfully identified by the suggested method and that it may be able to evade detection by widely used detectors currently in use.

The detection of anomalous behaviours, such as electricity theft, is made possible by analysing the current, voltage and electric energy data collected by the apparatus used to collect it. [10] Identify the vulnerabilities brought on by electricity theft by analysing the smart grid community's methods. As we have discovered, data-driven models may not be as useful when fictitious measurements deviate only slightly from ingrained normal usage patterns. Experimental findings demonstrate the recommended approach's ability to recognise the novel assault and its potential to avoid detection by currently in use, widely utilised detectors. [13] a sectionalising and tie-switching reconfigurable framework for managing energy in renewable microgrids based on machine learning. [14] Forecasting has significantly decreased attacks on electricity theft in AMI. Classification is done using the Adasyn approach to 93.7%, 92.6%, and 97%, respectively, to forecast and detect cyber-attacks with high accuracy [27].

Table 1. Displays the literature's results for supervised deep learning approaches

Techniques	Contributions	Validation metrics	Limitations
Hybrid Deep Neural Network [6]	To identify consumers who steal electricity on purpose, malicious consumers	Accuracy	No reliable Performance metric is used
Convolutional Neural Network (CNN) [7]	Use data to extract local and global features to detect electricity theft.	AUC	Data imbalance
LSTM [8] [14]	LSTM's internal architecture has been enhanced, which improves performance when matched to an original LSTM.	F1-score	Not robust
RUSBoost [19]	Better performance was attained when identifying NTL	MCC, F1-score	No parameter tuning
SOMTE[29]	The final layer of CNN uses RF to prevent local optima.	F1-score	High execution time

Table 2. Data explanation

Description	Values
Time required to collect the data	2016–2020
The percentage of dishonest customers	1592
number of loyal customers	8570
Overall clients	10,172
Real-world data	10%

Methods for balancing data Weighing, Random under Sampling (RUS), Random and Cluster-based Oversampling, and Logistic Regression are examples of machine learning techniques. [16] [17] Using the peak data (PEA), shoulder data (ARP), and sharp data (ARP), the power consumption record was described. Three input nodes were connected to one hidden neuron to create a basic network unit in the TSRNN architectural framework, which was used to extract data characteristics from the three defining variables. [28] TSRNN model automatically chooses the best values for these connecting weights based on the collected and simulated data.

A trained and optimised TSRNN model had a high discriminant accuracy of 95.1%. When the model was tested, its accuracy was found to be 89.3%. [19] The results of the simulation show that the suggested strategy solves the issues of data misbalancing, overfitting, and managing huge time series data. [29] An upgraded and improved random forest (RF) and synthetic minority oversampling technique (SMOTE) strategy serve as the cornerstones of a novel electricity theft detection system that has been suggested. The dataset was initially balanced using an enhanced SOMTE based on the K-means clustering technique.

2.1. Dataset Information

The largest utility in China, SGCC, provides information on electricity theft. The information is based on information about electricity consumption. The information in this dataset is categorised as either honest or fraudulent. The samples are widely dispersed, and the distribution of the classes is unbalanced.

Pre-processing techniques are needed because the data also includes missing and incorrect values. The publicly available data also reveal information about the actual situation, from which it can be deduced that 9% of all customers stole electricity in China. In this country, this crime is a major issue. Table 2 displays a description of the data.

3. Methodology

The suggested model is divided into three sections: (1) data pre-processing, which computes missing values in the dataset using interpolation; (2) normalisation and passing to the following model for feature extraction; and (3) using the refined features to train the CNN. Using the Bi-LSTM classifier method, the theft is located, and regular electricity is found. A variety of performance measures are applied in comparative analysis. Our suggested model's effectiveness is verified using the F1-score, precision, recall, and accuracy.

Data processing and CNNs using Bi-LSTM-based deep learning models have been proposed as early detection strategies for power theft. Data processing in this method includes data selection, data normalisation, and weight update. Using the generated data set, a CNN was also trained and evaluated with the proposed Bi-based deep learning model. Figure 1 shows the proposed ETD system model.

3.1. Pre-Processing

Pre-processing of the data is necessary because actual data on electricity consumption is frequently incomplete and unreliable. A variety of missing and incorrect numbers can be found in the raw data gathered from the SGCC as a result of the use of defective measurement techniques, such as smart metre technology or inaccurate transmission. We employ two procedures in this paper's data pre-processing stage to recover missing values: data interpolation and a data normalisation method.

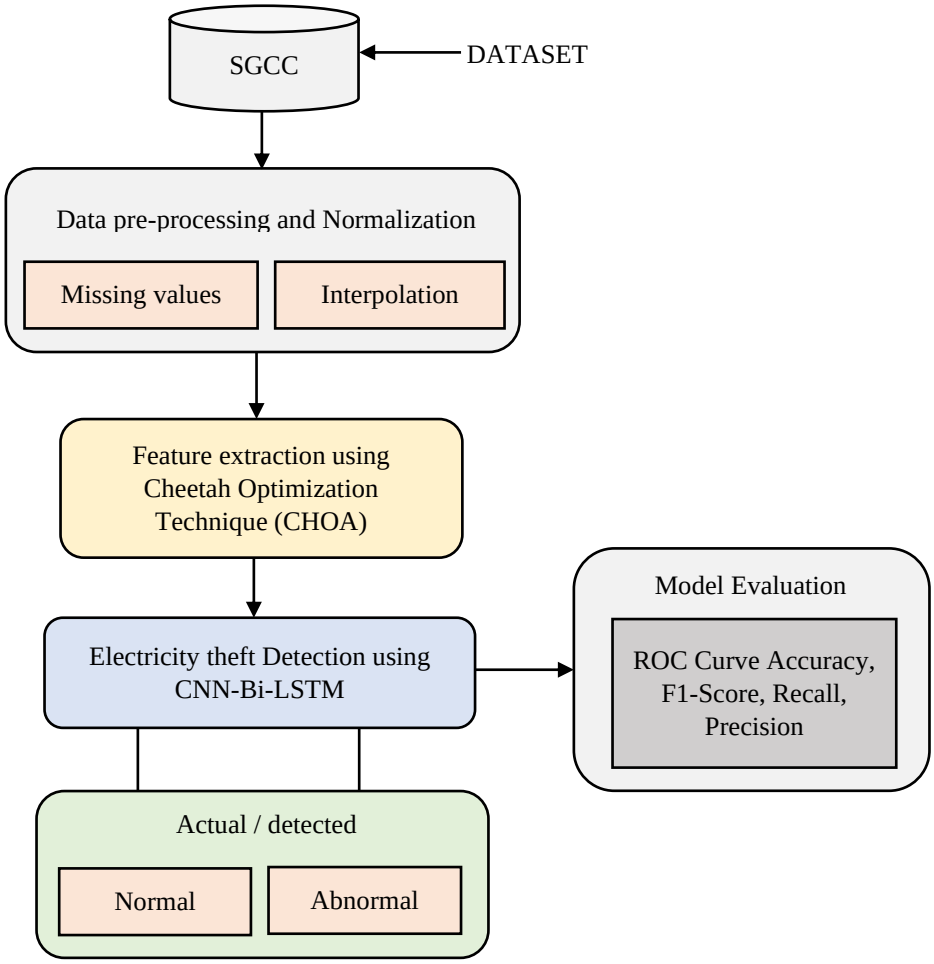

Fig. 1 Proposed ETD block diagram

3.1.1. Data Interpolation

Missing Values:

In order to compute the missing values, our suggested pre-processing algorithm uses the local average of power consumption. Our approach to recovering missing values for a particular day (for example, Monday) is shown in equation 1. If the missing value is not in the C_{Mi} position.

$$f(C_{Mi}) = \begin{cases} \frac{\sum_{n=1}^{x} CM_n}{n} & 1 \le n \le 4, n \in N \\ C_{Mi} & M_i \notin N_a N \\ -1 & n = 0 \end{cases} \quad (1)$$

The electricity consumed in this example is C_{Mi} on the I[th] Monday of a certain month (there are four or five Mondays in a month). In that particular month, CMn stands for the total amount consumed on all other Mondays.

3.1.2. Data Normalisation

The data on electricity consumption must be normalised after the missing values and outliers have been removed because the neural network is sensitive to various data. Last but not least, the dataset is normalised to lessen the sensitivity of CNN to dataset diversity. Min-max scaling formula shown in Equation 2 is what we use to prepare our data.

$$F(x_{i,t}) = \frac{x_{i,t} - min(x_{i,T})}{max(x_{i,T}) - min(x_{i,T})} \quad (2)$$

Where the numbers $min(x_{i,T})$ and m$max(x_{i,T})$re reflect a minimum and maximum value for a day, respectively.

3.2. Extraction using Modified Cheetah Optimization Technique (MCHOA)

The original data features, such as related and abnormal power theft data, were successfully extracted using the modified Cheetah optimisation method by pre-processing the sample data in the model performance data input step. Then, to identify electricity theft, we classify the output samples using the Modified Cheetah Optimization (MCHOA) method and create a diagnostic behavioural model of EV charging station users.

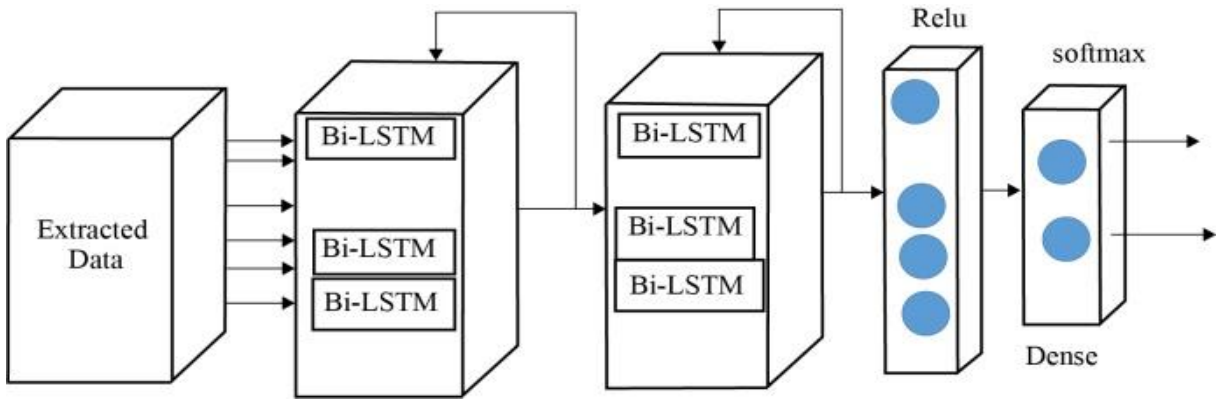

Fig. 2 Proposed CNN with Bi-LSTM model

3.2.1. Feature Extraction

After data normalisation, abnormal samples were added to the original dataset in accordance with the equations in [3] to achieve a balance between abnormal and normal samples of the dataset and boost the rate of accurate theft detection.

$$velocity_{cheetah_i} = \omega * velocity_{cheetah_i} + rand1() * \alpha * \left(location_{victim} - location_{cheetah_i}\right) \quad (3)$$

In order to protect customers' privacy, the sampling frequency and hourly metre readings have been reduced. Six such simulated attacks are produced for each sample with sample$x = \{x_1, \ldots, x_t \quad t = 1,2, \ldots,24\}$, as follows:

$$h_1(x_t) = \alpha x_t \quad (4)$$

$$h_2(x_t) = y_t x_t \quad (5)$$

Function $h_1(x_t)$ multiplies each sample individually in a different random value during the function $h_2(x_t)$ multiplies all samples collectively in a single random value.

3.2.2. Feature Selection

Feature selection is a dimension reduction approach used in machine learning, data mining, pattern recognition, and other fields. In actuality, feature selection increases prediction accuracy by choosing an efficient feature subset from an initial feature set. The majority of the features in a dataset are redundant, unimportant, or noisy. Eliminating these features while keeping the crucial ones increases learning effectiveness and decreases computational costs. Although numerous approaches to the issue of choosing important features have been put forth, the majority of these suffer from the issues of high complexity, high computational cost, and early convergence. Due to the increased interest in using meta-heuristic algorithms to overcome these problems, they are now among the most effective techniques and can extract the optimal subset of characteristics.

The Modified CHOA method is recommended for feature selection in this paper due to its exceptional performance in assuring diversity and intensification as well as the utilisation of the dynamic Attention factor for each cheetah. The binary string $F = \{F_1, F_i \ldots, F_n \quad n = 1,2, \ldots,2\}$ is used to represent each cheetah. The consumption for the hour the customer sends to the centre is specified by Fi. The features' values are taken into consideration between 0 and 1. If the appropriate bit value is more than 0.5, the feature is picked; if it is less than 0.5, the feature is not selected.

Each cheetah actually represents a subset of attributes that is a potential solution. Each cheetah's fitness is assessed using base classifiers, and the cheetah with the highest fitness is chosen as the$\text{cheetah}_{\text{Leader}}$. The location vector for the cheetah leader is saved, and the cheetah Leader has updated if the fitness of the cheetah is higher than that of the cheetah Leader. The $\text{cheetah}_{\text{Leader}}$best features for each base classifier are finally retrieved after satisfying the algorithm termination conditions.

3.3. Electricity Theft Detection based on CNN with BI-LSTM

A method for early power theft detection using CNNs with Bi-LSTM-based deep learning and data processing models have been proposed. The normalisation, selection, and update of weights are all components of this data processing method. With the help of the created dataset, the proposed LSTM-based deep learning model was also trained and tested. Figure 2 presents a block diagram of the proposed procedure.

3.3.1. CNN with Bi-LSTM

To assess the effectiveness of this study, an LSTM-based model was created. A key component of the LSTM model is a cellular memory RNN that outperforms a DNN system for classifying speech and signal data. Input control requires the validation of input memory locations. The output memory location is also checked to regulate output flow to the LSTM block.

An input layer is followed by bi-LSTM cells. After processing the data in Bi-LSTM cells with 64-digit weights, a 20% dropout layer was utilised to minimise the amount of data generated. Another attempt was made to use flat layers to bring neurons from earlier Bi-LSTM cells into one dimension and dropout layers to stop overfeeding.

Following that, a softmax classifier with dense layers is fed with all of the parameters. Use this layer to describe the various data classes that make up the dataset thoroughly. The proposed CNN and an overview of the Bi-LSTM model's parameters are shown in Figure 2.

The hidden stateh_t, forget gatef_t, memory gatei_t, and output gateot. Make up the Bi-LSTM model. It also has an inputx_t, a cell state$\overline{C_t}$, a temporary cell stateC_t, and a hidden state at time t.

$$f_t = \sigma\left(W_f.[h_{t-1}, x_t] + b_f\right) \quad (6)$$

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \quad (7)$$

$$\overline{C_t} = tanh(W_c.[h_{t-1}, x_t] + b_c) \quad (8)$$

Forgetting gate f_t the memory gate i_t, and an output gateot. Which control forgettingh_t, memory, and output accordingly, are calculated at each time step using an implicit state h_{t-1} at t.

$$C_t = f_t * C_{t-1} * i_t * C_t \quad (9)$$

$$ot = \sigma(W_o.[h_{t-1}, x_t] + b_o) \quad (10)$$

$$h_t = 0t * tanh(C_t) \quad (11)$$

To transmit valuable information to x t for additional calculation moments and discard useless information, the computational method of Bi-LSTM can be summarised as forgetting information from a cell state and remembering new knowledge. The overall framework and memory changes are determined for each time step t using the following formulas: The letters i_t,f_t, ot,C_t, and h_t in the preceding equation stand in for the terms input gates, output gates, hidden states, oblivion gates, and storage cells, respectively. The result of the elements is indicated by the asterisk (*). The other parameters are weight matrices, which need to be understood and communicated between all-time stages.

4. Experimental Results

The simulations have been conducted on a platform with a 4 GB RAM Intel Core i5 processor. We performed the simulations on the normalisation and interpolation-pre-processed data set. The SGCC dataset was used to train the proposed model. Use pre-processing data procedures to prepare data for model training and remove unnecessary data. The modified Cheetah Optimisation Method (MCHOA) is used to select suitable features for the underlying classifier while the model analyses the measured voltage, current, and electrical energy. After the feature extraction step is complete, the extracted data is classified using the proposed CNN with Bi-LSTM. The data from a metre, including the metre ID, the amount of energy consumed each hour (in kWh), and the date of consumption supplied to the centre, is shown in Table 3.

4.1. Performance Metrics

F1-score, recall, and precision is a few performance metrics considered when evaluating the suggested model's performance. The loss and accuracy of training and testing are also calculated to assess the efficacy of the suggested and reference models. Table 4 shows the metrics used to evaluate the proposed model.

4.1.1. Accuracy and F1 Score

Accuracy is defined as the ratio of all samples to the anticipated number of properly expected results by the model.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{Total}} \quad (12)$$

Also known as the F measure. The model test accuracy is determined, and test scores are evaluated using recall and accuracy. The following equation is used to evaluate the F1 score.

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (13)$$

4.1.2. Precision and Recall

Accuracy demonstrates consistency across all observed outcomes. Calculating accuracy involves dividing the total true positives by the sum of true positives and false positives. An equation includes this.

$$\text{Recall} = \frac{\text{True positive}}{\text{True Positive+False positive}} \quad (14)$$

Recall refers to the number of actual positive outcomes found relative to the expected outcome. Recall can be calculated by dividing the sum of true positives and false negatives by the total number of true positives. The equation gives

$$\text{Recall} = \frac{\text{True positive}}{\text{True Positive+False Negative}} \quad (15)$$

Recall counts a true positive across all classifier's outputs. Correctly categorised electricity steel thieves are considered true positives. False-positive means that law-abiding electricity users were mistakenly labelled as thieves.

Table 3. Consumption information of a meter

Date	Hour 1 (kWh)	Hour 24 (kWh)	Meter ID
8/29/2009	0.159	0.098	1284

Table 4. Performance metrics score

Techniques	F1-Score	Precision	Recall
SVM	82.5%	86.2%	88.2%
RNN	86.2%	85.1%	86.78%
RF	91.1 %	93.3%	95.3%
MCHOA	95.1%	94.3%	97.7%

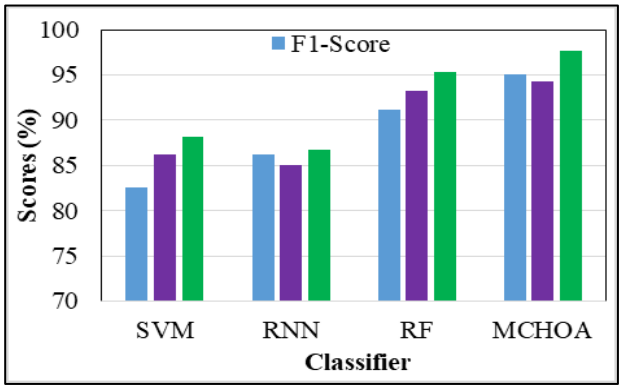

Fig. 3 Performance comparison

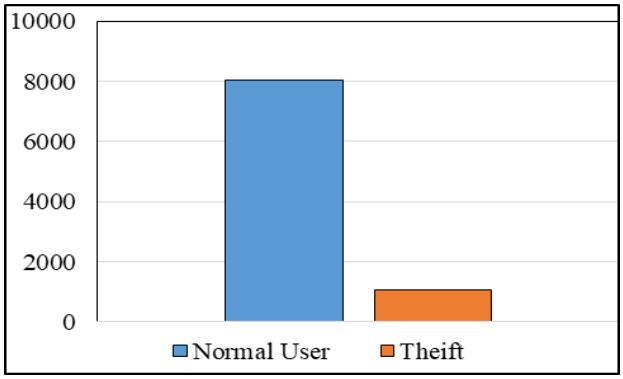

Fig. 4 Distribution of normal and theft users in the dataset

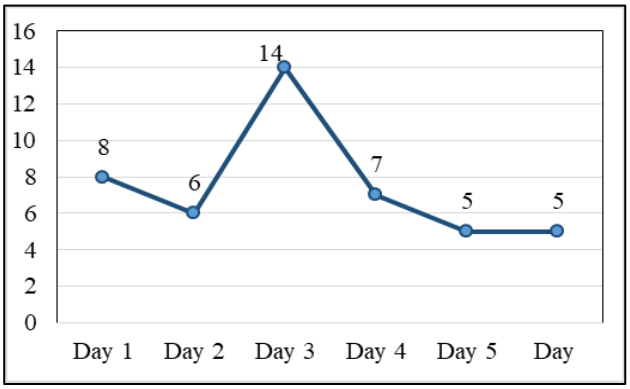

Fig. 5 Theft user

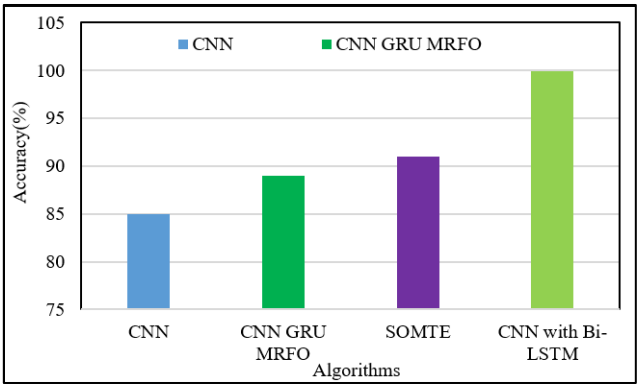

Fig. 6 Proposed method

True negative means that honest consumers were correctly classified as such, whereas false negative means that energy thieves were falsely labelled. As opposed to precision, which gauges how relevant a classifier's findings are. A high level of precision indicates that the relevant results of the classifier outweigh the irrelevant ones.

The performance of random forest is poor, as shown in Figure 3, and it is unable to accurately categorise people who have engaged in fraud as a result of training using unbalanced data. Compared to the random forest, the outcomes using the Modified Cheetah Optimization Technique (MCHOA) approach are better, and the synthetic data are not an accurate representation of actual theft situations. Our suggested solution outperforms them all for the unbalanced dataset compared to other methods.

An imbalanced dataset is one in which one class has significantly more instances than the other, as is the case with the dataset on electricity theft. Figure 4 depicts the distribution of two types of users: normal users and stealers. Distribution demonstrates that, in relation to the total number of users, the proportion of people who steal is incredibly low.

The weekly usage for theft users is shown in Figure 5. A thief's consumption habits are different from those of an ordinary consumer.

As seen in Figure 6, our improved method outperforms CNN with Bi-LSTM. In comparison to CNN-GRU and SMOTE, CNN's accuracy with Bi-LSTM is 99.8%, which is 6% and 11% higher, respectively.

5. Conclusion

In order to identify electricity theft, a unique CNN-RF model is described in this study. The suggested system pre-processes electrical data to remove nulls and nulls using normalisation and interpolation techniques. The necessary features are then extracted from the pre-processed data using Modified Cheetah Optimization Technique for feature refining. Finally, the data is classified into honest and

dishonest customers using a CNN with a Bi-LSTM approach. We evaluate the performance of SVM, RF, and RNN models by comparing them with the proposed model. An estimation simulation showed that the suggested model outperformed a previous model in terms of maximising parameters, handling imbalanced data, and avoiding overfitting. The suggested model also achieves 87.9% using performance measures, 88.9% for precision, 91.09% for recall, and 96.1% for F1-score. Future considerations would include power datasets for both residential and commercial structures.

References

[1] Rui Xia et al., "An Efficient Method Combined Data-Driven for Detecting Electricity Theft with Stacking Structure Based on Grey Relation Analysis," *Energies*, vol. 15, no. 9, p. 7423, 2022. [CrossRef]

[2] Hong-Xin Gao, Stefanie Kuenzel, and Xiao-Yu Zhang, "A Hybrid ConvLSTM-based Anomaly Detection Approach for Combating Energy Theft," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1-10, 2022. [CrossRef]

[3] Ayush Jain et al., "Detection of Sarcasm through Tone Analysis on video and Audio files: A Comparative Study on Ai Models Performance," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 12, pp. 1-5, 2021. [CrossRef]

[4] Rui Xia et al., "A Fast and Efficient Method Combined Data-Driven for Detecting Electricity Theft to Secure the Smart Grid with Stacking Structure," *SSRN*, 2022. [CrossRef]

[5] Madhuri V. Joseph, "Sentiment Analysis of Amazon Review using Improvised Conditional Based Convolutional Neural Network and Word Embedding," *International Journal of Engineering Trends and Technology*, vol. 70, no. 12, pp. 194-209, 2022. [CrossRef]

[6] Ashraf Ullah et al., "A Hybrid Deep Neural Network for Electricity Theft Detection using Intelligent Antenna-Based Smart Meters," *Wireless Communications and Mobile Computing*, 2021. [CrossRef]

[7] Jeanne Pereira, and Filipe Saraiva, "Convolutional Neural Network Applied to Detect Electricity Theft: A Comparative Study on Unbalanced Data Handling Techniques," *International Journal of Electrical Power & Energy Systems*. [CrossRef]

[8] Yuan Shen et al., "An Identification Method of Anti-Electricity Theft Load Based on Long and Short-Term Memory Network," *Procedia Computer Science*, vol. 183, pp. 440-447, 2021. [CrossRef]

[9] M. Preethi, C. Velayutham, and S. Arumugaperumal, "A Novel RGB Channel Assimilation for Hyperspectral Image Classification using 3D-Convolutional Neural Network with Bi-Long Short-Term Memory," *International Journal of Engineering Trends and Technology*, vol. 70, no. 3, pp. 201-211, 2022. [CrossRef]

[10] Lei Cui et al., "A Covert Electricity-Theft Cyber-Attack against Machine Learning-Based Detection Models," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7824-7833, 2022. [CrossRef]

[11] Guixue Cheng et al., "Energy Theft Detection in an Edge Data Center using Deep Learning," *Mathematical Problems in Engineering*, 2021. [CrossRef]

[12] Ms.S.Supraja, and Dr.P.Ranjith Kumar, "An Intelligent Traffic Signal Detection System Using Deep Learning," *SSRG International Journal of VLSI & Signal Processing*, vol. 8, no. 1, pp. 5-9, 2021. [CrossRef]

[13] Tianze Lan et al., "An Advanced Machine Learning Based Energy Management of Renewable Microgrids Considering Hybrid Electric Vehicles Charging Demand," *Energies*, vol. 14, no. 3, pp. 569, 2021. [CrossRef]

[14] Rutuja Umesh Madhure, Radha Raman, and Sandeep Kumar Singh, "CNN-LSTM based Electricity Theft Detector in Advanced Metering Infrastructure," *2020 11th International Conference on Computing, Communication and Networking Technologies*, pp. 1-6, 2020. [CrossRef]

[15] Dr.V.V.Narendra Kumar, and T.Satish Kumar, "Smarter Artificial Intelligence with Deep Learning," *SSRG International Journal of Computer Science and Engineering*, vol. 5, no. 6, pp. 10-16, 2018. [CrossRef]

[16] Jeanne Pereira, and Filipe Saraiva, "A Comparative Analysis of Unbalanced Data Handling Techniques for Machine Learning Algorithms to Electricity Theft Detection," *2020 IEEE Congress on Evolutionary Computation*, pp. 1-8, 2020. [CrossRef]

[17] Guoying Lin et al., "Electricity Theft Detection in Power Consumption Data Based on Adaptive Tuning Recurrent Neural Network," *Frontiers in Energy Research*, vol. 9, p. 773805, 2021. [CrossRef]

[18] M.Muruga Lakshmi, and Dr.S.Thayammal, "Ship Detection in Medium-Resolution SAR Images using Deep learning," *SSRG International Journal of Electronics and Communication Engineering*, vol. 8, no. 5, pp. 1-5, 2021. [CrossRef]

[19] Muhammad Adil et al., "LSTM and Bat-Based RUSBoost Approach for Electricity Theft Detection," *Applied Sciences*, vol. 10, no. 12, p. 4378, 2020. [CrossRef]

[20] D. J. Samatha Naidu, and R. Lokesh, "Missing Child Identification System using Deep Learning with VGG-FACE Recognition Technique," *SSRG International Journal of Computer Science and Engineering*, vol. 9, no. 9, pp. 1-11, 2022. [CrossRef]

[21] Murthy V. S. N. Tatavarthy, and V. Naga Lakshmi, "Pedagogical Content Knowledge Classification using CNN with Bi-LSTM," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 264-271, 2022. [CrossRef]

[22] Junhao Shi et al., "A Novel Approach to Detect Electricity Theft Based on Conv-Attentional Transformer," *SSRN*, 2022. [CrossRef]

[23] Joyassree Sen et al., "Face Recognition using Deep Convolutional Network and One-shot Learning," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 4, pp. 23-29, 2020. [CrossRef]

[24] Yanlin Peng et al., “Electricity Theft Detection in AMI Based on Clustering and Local Outlier Factor,” *IEEE Access*, vol. 9, pp. 107250-107259, 2021. [CrossRef]

[25] Shahriar Rahman Fahim et al., “A Deep Learning Based Intelligent Approach in Detection and Classification of Transmission Line Faults,” *International Journal of Electrical Power & Energy Systems*, vol. 133, p. 107102, 2021. [CrossRef]

[26] Zhuang Yuan, and Wu Chunrong, "Deep Learning-Based Listening Teaching Strategy in Junior Middle School," *SSRG International Journal of Humanities and Social Science*, vol. 9, no. 2, pp. 65-70, 2022. [CrossRef]

[27] Zahoor Ali Khan et al., “Electricity Theft Detection Using Supervised Learning Techniques on Smart Meter Data,” *Sustainability*, vol. 12, no. 19, p. 8023, 2020. [CrossRef]

[28] Anupam Das, and Adian McFarlane, “Non-Linear Dynamics of Electric Power Losses, Electricity Consumption, and GDP in Jamaica,” *Energy Economics*, vol. 84, p. 104590, 2019. [CrossRef]

[29] Zhengwei Qu et al., “Detection of Electricity Theft Behavior Based on Improved Synthetic Minority Oversampling Technique and Random Forest Classifier,” *Energies*, vol. 13, no. 8, p. 2039, 2020. [CrossRef]

[30] Shoaib Munawar et al., "Electricity Theft Detection in Smart Grids Using a Hybrid BiGRU–BiLSTM Model with Feature Engineering-Based Preprocessing," *Sensors*, vol. 22, no. 20, p. 7818, 2022. [CrossRef]