ELECTRICITY ENERGY THEFT DETECTION IN SMART GRIDS USING DEEP NEURAL NETWORKS

B Hussain 1,Arcot Naveen2,Lambade Venkatesh3,Jujare Ranjith Kumar4,D K Krishna Mohan5,M Vinod Kumar6,M Ravi Kiran7

1 Asst Prof, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail:himajareddy73@gmail.com

2UG Scholar, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail:arcotnaveen234@gmail.com

3UG Scholar, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail: lvenkat0712@gmail.com

4UG Scholar, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail: akashifahmed31@gmail.com

5 UG Scholar, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail: mohankrishnaa1234@gmail.com

6UG Scholar, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail:vinu7095920919@gmail.com

7UG Scholar, Dept of CSE, Bheema college of Engineering and Technology, Dhanapuram, AP, India,

E-mail:chinniravi2001@gmail.com

**ABSTRACT**

Electricity theft poses a significant challenge globally, impacting both utility companies and consumers. It hampers the financial stability of utility providers, poses safety risks, and contributes to the high cost of energy for consumers. The advent of smart grid technology presents an opportunity to combat this issue by leveraging vast amounts of data, including customer consumption patterns, which can be analyzed using machine learning and deep learning methods to identify instances of theft. This study introduces a novel approach to theft detection employing a deep neural network, incorporating a wide range of features extracted from both temporal and frequency domains. To address limitations in the dataset such as missing data and class imbalances, techniques like data interpolation and synthetic data generation are employed. The study explores the significance of features from both domains, conducts experiments with reduced feature sets using principal component analysis, and employs a minimum redundancy maximum relevance scheme to identify key features. Performance optimization is achieved through hyperparameter tuning using a Bayesian optimizer and experimentation with different parameter values using an adaptive moment estimation optimizer. Results demonstrate the effectiveness of the proposed method, with a 97% area under the curve (AUC) and 91.8% accuracy, surpassing previous benchmarks in theft detection accuracy.

**INTRODUCTION**

Introduction to Electricity Energy theft detection in Smart Grids using Deep Neural Networks:

The Problem:

Electricity theft poses a significant challenge for energy providers worldwide, resulting in substantial financial losses, with estimates exceeding $96 billion annually due to Non-Technical Losses (NTLs), where electricity energy theft plays a major role

. In sub-Saharan Africa alone, approximately half of the energy generated is unlawfully taken [2]. The primary aim of electricity thieves is to consume electricity without being properly billed or to pay less than the actual amount consumed, leading to substantial revenue losses for utility companies. For instance, in 2015, India, Brazil, and Russia reported losses of $16.2 billion, $10.5 billion, and $5.1 billion, respectively [5]. South Africa, through its utility Eskom, suffers an estimated annual revenue loss of $1.31 billion (R20 billion) due to electricity energy theft [2].

Beyond financial implications, electricity energy theft directly impacts the stability and reliability of power grids, causing issues like surges, overloads, and safety hazards such as electric shocks [4]. Moreover, it contributes to energy tariff increases, affecting all consumers. Addressing this issue, many utilities have turned to smart grid technologies, integrating traditional grids with smart meters and sensors connected through communication networks [6]. These smart devices collect data on electricity usage, grid status, and pricing, offering opportunities to combat theft more effectively.

Traditionally, utilities have attempted to combat theft through meter inspections and power line checks, but these methods are costly, inefficient, and ineffective against cyber threats [4], [7]. Recent efforts have focused on utilizing machine learning classification techniques, leveraging smart meter data to detect theft more affordably [8]. However, existing methods often overlook frequency-domain features, limiting their effectiveness.

Despite ongoing research, electricity energy theft remains a persistent problem, exacerbated by the slower adoption of smart grid technologies in developing nations due to infrastructure limitations and privacy concerns [9], [10]. Nonetheless, smart meters are gaining traction globally, with developed and developing countries alike considering their deployment to address NTLs [10]. The smart grid market is projected to expand significantly, particularly in North America, Europe, and Asia [11].

In this study, we propose an advanced theft detection method based on deep neural networks, emphasizing the importance of incorporating both time-domain and frequency-domain features for improved classification performance. By leveraging frequency-domain features alongside traditional methods, we aim to enhance the accuracy and efficiency of electricity energy theft detection systems [2].

LITERATURE SURVEY

‘‘An alternative technique for the detection and mitigation of electricity theft in South Africa,’

Q. Louw and P. Bokoro

Electricity theft and illegal connection by ground surface conductors is a pervasive problem in South Africa. The impact this phenomenon has is not only limited to revenue loss and equipment damage, but also presents a life threatening hazard. Although the issues of non-technical losses have been researched for decades, no universal solution has been presented, due to the complexity of the problem. This paper investigates the application of zero-sequence current-based detection as a mitigation strategy to deal with illegal connections by ground surface conductors. Simulation and experimental results show the validity of this technique as well as its dependence on seasonal change of the soil resistivity.

‘‘Electricity theft detection using pipeline in machine learning,’’

M. Anwar, N. Javaid, A. Khalid, M. Imran, and M. Shoaib

Electricity energy theft is the primary cause of electrical power loss that significantly affects the revenue loss and the quality of electrical power. Nevertheless, the existing methods for the detection of this criminal behavior of theft are diversified and complicated since the imbalanced nature of the dataset, and high dimensionality of time-series data make it challenging to extract meaningful information. This paper addresses these problems by developing a novel electricity energy theft detection model, integrating three algorithms in a pipeline. The proposed method first applies the synthetic minority oversampling technique (SMOTE) for balancing the dataset, secondly integration of kernel function and principal component analysis (KPCA) for the feature extraction from high dimensional time-series data, and support vector machine (SVM) for the classification. Besides, the performance of the proposed pipeline is measured using a comprehensive list of performance metrics. Extensive experiments are performed by using real electricity consumption data, and results show that the proposed method outperforms other methods in terms of theft detection.

‘‘Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids,’’

Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou

Electricity theft is harmful to power grids. Integrating information flows with energy flows, smart grids can help to solve the problem of electricity theft owning to the availability of massive data generated from smart grids. The data analysis on the data of smart grids is helpful in detecting electricity theft because of the abnormal electricity consumption pattern of energy thieves. However, the existing methods have poor detection accuracy of electricity theft since most of them were conducted on one-dimensional (1-D) electricity consumption data and failed to capture the periodicity of electricity consumption. In this paper, we originally propose a novel electricity-theft detection method based on wide and deep convolutional neural networks (CNN) model to address the above concerns. In particular, wide and deep CNN model consists of two components: the wide component and the deep CNN component. The deep CNN component can accurately identify the nonperiodicity of electricity theft and the periodicity of normal electricity usage based on 2-D electricity consumption data. Meanwhile, the wide component can capture the global features of 1-D electricity consumption data. As a result, wide and deep CNN model can achieve the excellent performance in electricity-theft detection. Extensive experiments based on realistic dataset show that wide and deep CNN model outperforms other existing methods.

‘‘Smart grid—The new and improved power grid: A survey,’’

X. Fang, S. Misra, G. Xue, and D. Yang

The Smart Grid, regarded as the next generation power grid, uses two-way flows of electricity and information to create a widely distributed automated energy delivery network. In this article, we survey the literature till 2011 on the enabling technologies for the Smart Grid. We explore three major systems, namely the smart infrastructure system, the smart management system, and the smart protection system. We also propose possible future directions in each system. colorred{Specifically, for the smart infrastructure system, we explore the smart energy subsystem, the smart information subsystem, and the smart communication subsystem.} For the smart management system, we explore various management objectives, such as improving energy efficiency, profiling demand, maximizing utility, reducing cost, and controlling emission. We also explore various management methods to achieve these objectives. For the smart protection system, we explore various failure protection mechanisms which improve the reliability of the Smart Grid, and explore the security and privacy issues in the Smart Grid.

‘‘Machine learning techniques for energy theft detection in AMI,’’

A. Maamar and K. Benahmed

Advanced Metering Infrastructure (AMI and smart meter) is considered as the basic building block for the development of smart grid in the power distribution system. a Smart meter is one of the keys elements of Advanced Metering Infrastructure, it provides two-way communication between customer and electricity utility, Smart Meters send consumption data frequently (e.g., every 15 minutes) to the utility for monitoring and billing, therefore, a gold mine of data is generated for utilities. Smart meters have become a major focus for targeted attacks which lead to the energy theft, resulting in losses of billions of dollars per year in many countries. Therefore, multitude of papers have studied the energy theft detection by applying different disciplines on smart meter data. In this paper, we present an overview of machine learning research in energy theft detection using smart meter data. It then surveys these research efforts in a summary and comparison of learning models used, in terms of performance metrics, simulation and analysis environment, and data sets used. It finally highlights the challenges in energy theft detection. We approve that these challenges have not been adequately addressed and considered in previous contributions, also covering them, is necessary to advance the energy theft detection.

‘‘Progress and challenges in smart grids: Distributed generation, smart metering, energy storage and smart loads,’

I. Diahovchenko, M. Kolcun, Z. Čonka, V. Savkiv, and R. Mykhailyshyn

The future power system must provide electricity that is reliable and affordable. To meet this goal, both the electricity grid and the existing control system must become smarter. In this paper, some of the major issues and challenges of smart grid’s development are discussed, and ongoing and future trends are presented with the aim to provide a reader with an insight on the relevant research topics, challenges and actual engineering tasks in smart grids. The focus areas of this review study are distributed generation, microgrids, smart meters’ deployment, energy storage technologies, and the role of smart loads in primary frequency response provision. The exploration of smart grid technologies and distributed generation systems has been accomplished, and a general comparison of the conventional grid and a future smart model is included. The issue of increasing penetration of renewable energy sources to the power system and posers related to the integration of distributed generation are also presented.

‘‘Minimizing household electricity theft in Nigeria using GSM based prepaid meter,’’

D. O. Dike, U. A. Obiora, E. C. Nwokorie, and B. C. Dike

Many households indulge in different forms of electricity theft and illegal tampering of electric metering devices. These lead to distribution system faults and overload as well as loss of revenue by the distribution companies,this paper envisages the utilization of the global system for mobile communication (GSM) into the prepaid energy meter for increased generation of revenue in developing countries like Nigeria. The proposed meter is set to carry a unique identification number such as the consumer’s phone number which may be encrypted into the memory of the microcontroller. Electricity theft is being detected as the GSM module sends message to the distribution company. Revenue generated can be increased through the use of the proposed meter as unaccountability by utility workers and billing irregularities are eliminated. The results obtained from the simulation shows that immediately an illegal load is connected to the utility system either within the residential meter jurisdiction or otherwise stated, the GSM module alerts the utility company no matter how small the illegal load is.

‘‘Prototype development to detect electric theft using PIC18F452 microcontroller,’’

S. B. Yousaf, M. Jamil, M. Z. U. Rehman, A. Hassan, and S. O. G. Syed

This paper presents the development of a prototype to detect electric theft using PIC18F452. The proposed prototype is robust, adaptable, repairable and easy installable. It monitors the flow of charge from the phase line i.e. supply line, the neutral line and constantly compares them. Moreover, it shows real time flow of charge in the both phase line and the neutral line. It also represents the real time voltage and the power being supplied to the load. It is also fitted with an alarm system that sounds an alarm when there is any electric theft. The prototype was able to adapt to different kinds of attenuating voltages between 200-240 volts. It was tested at different loads and findings were inconsistent with the theoretical ones. What makes this device unique is that it can be fitted anywhere in any electrical system. It can be used as metering device. It can also be used as a smart grid surveillance device when used in collaboration with multiple devices of same or different kind.

SYSTEM ANALYSIS AND DESIGN

**EXISTING SYSTEM**

Hardware-based methods [13]\_[19] typically involve the installation of specialized microcontrollers, sensors, and circuits on power distribution lines to detect instances of electricity theft, particularly those involving physical tampering with distribution components like distribution lines and electricity meters. However, these methods are not capable of detecting cyber attacks, which involve manipulating energy consumption data through hacking electricity meters [7].

For example, in [13], an electricity meter was redesigned to incorporate components such as a Global System for Mobile Communications (GSM) module, a microcontroller, and an Electrically Erasable Programmable Read-Only Memory (EEPROM). Through simulation, the meter was able to send Short Message Service (SMS) notifications whenever an illegal load was detected by bypassing the meter. Similarly, authors in [16] utilized a GSM module, an ARM Cortex-M3 processor, and other hardware components to address electricity theft in various forms, including bypassing the phase line, meter tampering, and other unauthorized modifications. A prototype was developed and tested to detect and notify instances of theft via SMS.

In [17], researchers designed a smart meter based on the ADE7953 chip, which could detect current and voltage tampering as well as mechanical interference. The ADE7953 chip detected irregularities such as overvoltage, dropping voltage, and overcurrent, triggering an interrupt signal to the Microcontroller Unit (MCU) to report tampering. Mechanical tampering was addressed by connecting a tampering switch to the MCU, enabling it to send alarm signals upon detection of tampering. Testing involved various tampering scenarios, including connecting neutral and phase lines and bypassing the phase line, with a low probability of detection failure (2.13%).

In [15], a circuitry was designed using a step-down transformer, voltage divider circuit, microchip, and other components to detect theft by comparing forward current on the main phase line with reverse current on the neutral line. This circuitry, installed before the meter, detected bypassing attempts and sounded an alarm. Similarly, [14] introduced a circuit to detect bypassing of the meter, incorporating transformers, rectifiers, a microcontroller, GSM module, and other components. The GSM module notified operators via SMS upon detecting meter bypassing.

**Disadvantages**

* An existing system not implemented DNN-BASED ELECTRICITY THEFT DETECTION METHOD.
* An existing system not implemented Hyperbolic tangent activation function.

**SOLUTION:PROPOSED SYSTEM**

\_ Drawing from existing literature, we propose a novel approach to detecting electricity theft utilizing a Deep Neural Network (DNN) classification method, leveraging comprehensive time-domain features. Additionally, we suggest incorporating frequency-domain features to augment performance.

We utilize Principal Component Analysis (PCA) to conduct classification with a reduced feature space. By comparing results obtained with all input features, we aim to interpret outcomes and streamline future training procedures.

Moreover, we employ the Minimum Redundancy Maximum Relevance (mRMR) scheme to pinpoint the most significant features. This approach validates the importance of frequency-domain features over time-domain features in detecting electricity theft.

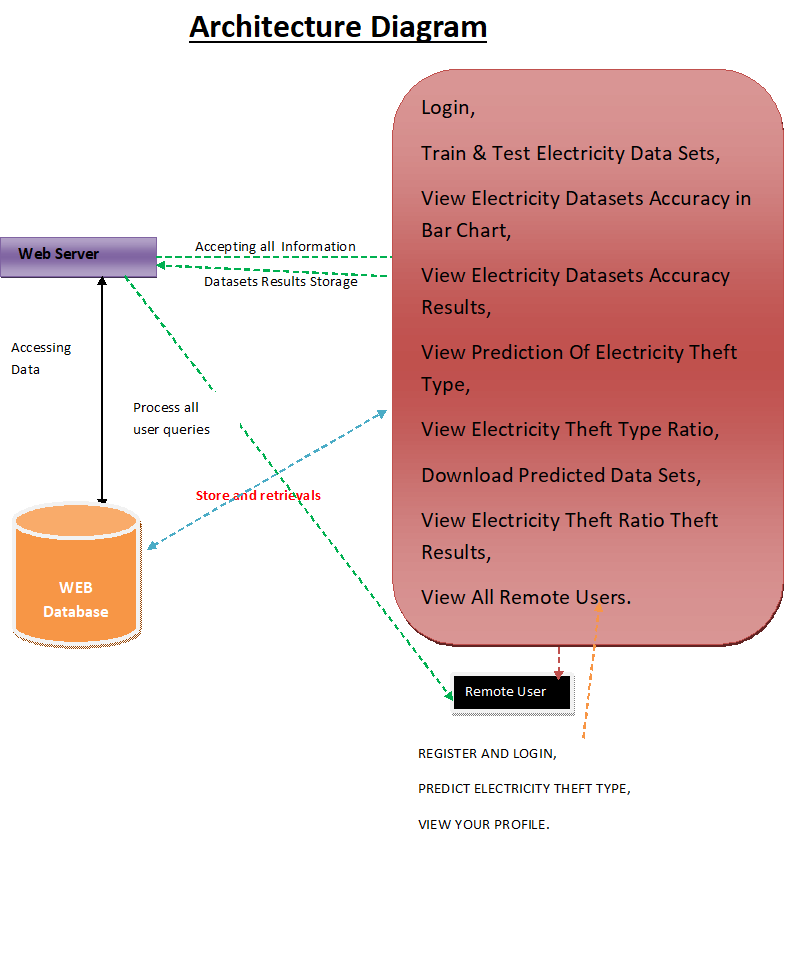
To enhance overall performance, we optimize the model's hyperparameters using a Bayesian optimizer. Additionally, we implement an adaptive moment estimation (Adam) optimizer to determine optimal ranges of values for other key parameters, thereby achieving efficient model training.

Finally, our findings demonstrate a 1% enhancement in Area Under the Curve (AUC) and competitive accuracy compared to other data-driven electricity theft detection methods documented in the literature, all evaluated on the same dataset.

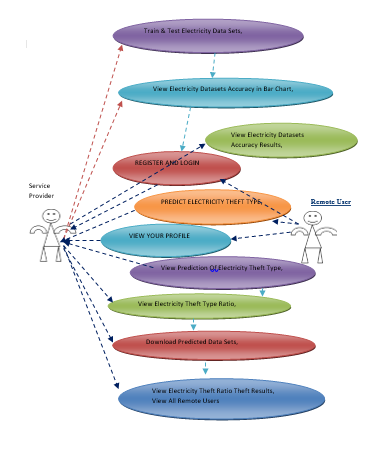
**Advantages**

* Huge amount of data obtained by cloud providers and other businesses, making large datasets that train DNNs effectively.
* Advances in machine learning and signal/information processing research which leads to the evolution of techniques to improve accuracy and broaden the domain ofDNNs application.

SYSTEM ARCHITECTURE

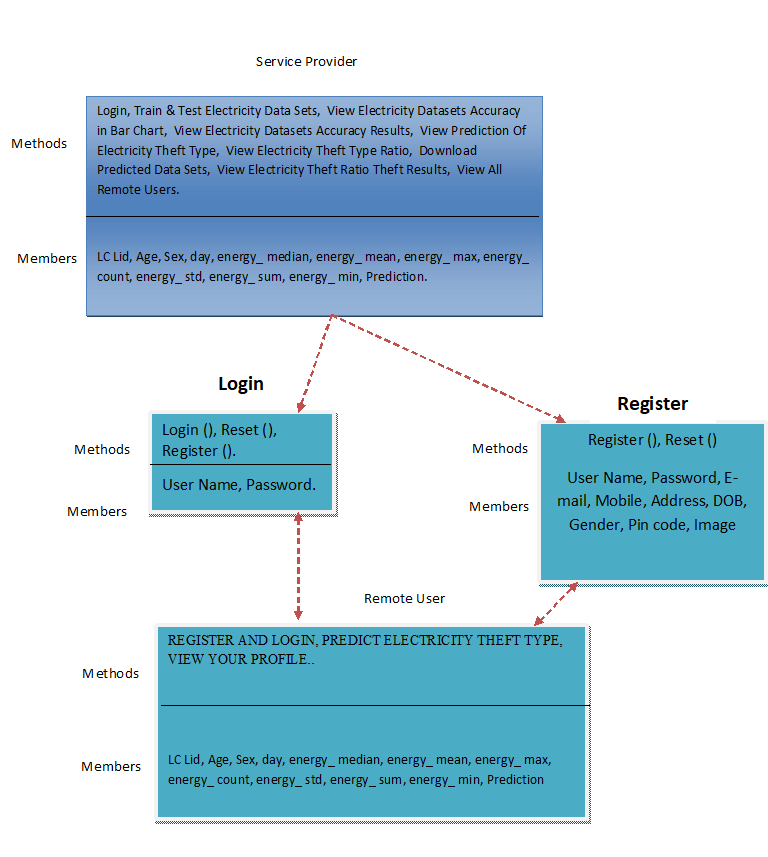


USE CASE DIAGRAM



CLASS DIAGRAM

.



IMPLEMENTATION

MODULES:

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such asLogin, Train & Test Electricity Data Sets, View Electricity Datasets Accuracy in Bar Chart, View Electricity Datasets Accuracy Results, View Prediction Of Electricity Theft Type, View Electricity Theft Type Ratio, Download Predicted Data Sets, View Electricity Theft Ratio Theft Results, View All Remote Users. View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user’s details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT ELECTRICITY THEFT TYPE,VIEW YOUR PROFILE

SYSTEM REQUIREMENTS

➢H/W SystemConfiguration:-

➢Processor - Pentium–IV

➢RAM - 4 GB(min)

➢Hard Disk - 20 GB

➢KeyBoard - Standard Windows Keyboard

➢Mouse - Two or ThreeButton Mouse

➢Monitor - SVGA

SOFTWARE REQUIREMENTS:

Operating system : Windows 7 Ultimate.

Coding Language : Python.

Front-End : Python.

Back-End : Django-ORM

Designing : Html, css, javascript.

Data Base : MySQL (WAMP Server).

Future Enhancement

1. Integrate multi-modal data, including weather and customer behavior; apply advanced signal processing for feature extraction.

2. Handle missing data with robust imputation and address dynamic class imbalance through effective methods.

3. Enable real-time theft detection by adapting models with new patterns through online learning.

4. Continuously benchmark performance against other methods and incorporate latest ML/DL advancements.

Conclusion

This study investigated electricity energy theft detection in smart grids using time-domain and frequency-domain features in a DNN-based classification approach. We compared isolated classification tasks based on these features and found that classification with frequency-domain features outperformed time-domain features, while combined domain features yielded the best results. With PCA feature reduction, the classifier achieved 85.8% accuracy and 92% AUC-ROC using 7 out of 20 components. MRMR analysis confirmed the importance of frequency-domain features. Bayesian optimization improved accuracy by nearly 1%, achieving 97% AUC. Our method outperformed existing data-driven methods with 91.8% accuracy. It can be applied beyond power distribution networks and extended for real-time theft detection. Further validation against diverse datasets is recommended for broader applicability.

REFERENCES

[1] S. Foster. (Nov. 2, 2021). Non-Technical Losses: A $96 BillionGlobal Opportunity for Electrical Utilities. [Online]. Available:https://energycentral.com/c/pip/ non-technical-losses-96-billion-globalopportunity-electrical-utilities

[2] Q. Louw and P. Bokoro, ``An alternative technique for the detection andmitigation of electricity energy theft in South Africa,'' SAIEE Afr. Res. J., vol. 110,no. 4, pp. 209\_216, Dec. 2019.

[3] M. Anwar, N. Javaid, A. Khalid, M. Imran, and M. Shoaib, ``Electricitytheft detection using pipeline in machine learning,'' in Proc. Int. WirelessCommun. Mobile Comput. (IWCMC), Jun. 2020, pp. 2138\_2142.

[4] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, ``Wide and deepconvolutional neural networks for electricity-theft detection to securesmart grids,'' IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 1606\_1615,Apr. 2018.

[5] P. Pickering. (Nov. 1, 2021). E-Meters Offer Multiple Ways toCombat Electricity Theft and Tampering. [Online]. Available:https://www.electronicdesign.com/technologies/meters

[6] X. Fang, S. Misra, G. Xue, and D. Yang, ``Smart grid\_The new andimproved power grid: A survey,'' IEEE Commun. Surveys Tuts., vol. 14,no. 4, pp. 944\_980, 4th Quart., 2012.

[7] M. Ismail, M. Shahin, M. F. Shaaban, E. Serpedin, and K. Qaraqe, ``Efficient detection of electricity theft cyber attacks in AMI networks,'' in Proc.IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1\_6.

[8] A. Maamar and K. Benahmed, ``Machine learning techniques for energytheft detection in AMI,'' in Proc. Int. Conf. Softw. Eng. Inf. Manage.(ICSIM), 2018, pp. 57\_62.

[9] A. Jindal, A. Schaeffer-Filho, A. K. Marnerides, P. Smith, A. Mauthe, andL. Granville, ``Tackling energy theft in smart grids through data-drivenanalysis,'' in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2020,pp. 410\_414.

[10] I. Diahovchenko, M. Kolcun, Z. .onka, V. Savkiv, and R. Mykhailyshyn,``Progress and challenges in smart grids: Distributed generation, smartmetering, energy storage and smart loads,'' Iranian J. Sci. Technol., Trans.Electr. Eng., vol. 44, no. 4, pp. 1319\_1333, Dec. 2020.

[11] M. Jaganmohan. (Mar. 3, 2022). Global Smart GridMarket Size by Region 2017\_2023. [Online]. Available:https://www.statista.com/statistics/246154/global-smart-grid-marketsize-

by-region/

[12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou.(Sep. 30, 2021). Electricity Theft Detection, [Online]. Available:https://github.com/henryRDlab/ ElectricityTheftDetection

[13] D. O. Dike, U. A. Obiora, E. C. Nwokorie, and B. C. Dike, ``Minimizinghousehold electricity theft in Nigeria using GSM based prepaid meter,''Amer. J. Eng. Res., vol. 4, no. 1, pp. 59\_69, 2015.

[14] P. Dhokane, M. Sanap, P. Anpat, J. Ghuge, and P. Talole, ``Power theftdetection & initimate energy meter information through SMS with autopower cut off,'' Int. J. Current Res. Embedded Syst. VLSI Technol., vol. 2,no. 1, pp. 1\_8, 2017.

[15] S. B. Yousaf, M. Jamil, M. Z. U. Rehman, A. Hassan, and S. O. G. Syed,``Prototype development to detect electric theft using PIC18F452 microcontroller,''Indian J. Sci. Technol., vol. 9, no. 46, pp. 1\_5, Dec. 2016.

[16] K. Dineshkumar, P. Ramanathan, and S. Ramasamy, ``Development ofARM processor based electricity theft control system using GSM network,''in Proc. Int. Conf. Circuits, Power Comput. Technol. (ICCPCT),Mar. 2015, pp. 1\_6.

[17] S. Ngamchuen and C. Pirak, ``Smart anti-tampering algorithm design forsingle phase smart meter applied to AMI systems,'' in Proc. 10th Int. Conf.Electr. Eng./Electron., Comput., Telecommun. Inf. Technol., May 2013,pp. 1\_6.

[18] B. Khoo and Y. Cheng, ``Using RFID for anti-theft in a Chinese electricalsupply company: A cost-bene\_t analysis,'' in Proc. Wireless Telecommun.Symp. (WTS), Apr. 2011, pp. 1\_6.

[19] J. Astronomo, M. D. Dayrit, C. Edjic, and E. R. T. Regidor, ``Developmentof electricity theft detector with GSM module and alarm system,'' in Proc.IEEE 12th Int. Conf. Humanoid, Nanotechnol., Inf. Technol., Commun.Control, Environ., Manage. (HNICEM), Dec. 2020, pp. 1\_5.

[20] P. Jokar, N. Arianpoo, and V. C. M. Leung, ``Electricity theft detection inAMI using customers' consumption patterns,'' IEEE Trans. Smart Grid,vol. 7, no. 1, pp. 216\_226, Jan. 2015.

[21] W. Han and Y. Xiao, ``A novel detector to detect colluded non-technicalloss frauds in smart grid,'' Comput. Netw., vol. 117, pp. 19\_31, Apr. 2017.

[22] S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, ``Electricity theft detectionusing smart meter data,'' in Proc. IEEE Power Energy Soc. Innov. SmartGrid Technol. Conf. (ISGT), Feb. 2015, pp. 1\_5.

[23] S. K. Singh, R. Bose, and A. Joshi, ``PCA based electricity theft detectionin advanced metering infrastructure,'' in Proc. 7th Int. Conf. Power Syst.(ICPS), Dec. 2017, pp. 441\_445.

[24] M. Di Martino, F. Decia, J. Molinelli, and A. Fernández, ``Improving electricfraud detection using class imbalance strategies,'' in Proc. ICPRAM,2012, pp. 135\_141.

[25] M. 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 basedapproach,'' Energies, vol. 12, no. 17, p. 3310, 2019.