International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

pp. 218-222, April

Intelligent Power Monitoring and Theft Detection System

U.Jeyamalar[1], V.Gayathri[2], K.Jayasri[3], R.Kanimozhi[4]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Kings College of Engineering Pudukottai.
ujeyamalar@gmail.com
[2]Student, Department of Electronics and Communication Engineering, Kings College of Engineering, Pudukottai.
gayathriveeraiyan556@gmail.com
[3]Student, Department of Electronics and Communication Engineering, Kings College of Engineering, Pudukottai.
jayasrik200407@gmail.com
[4]Student, Department of Electronics and Communication Engineering, Kings College of Engineering, Pudukottai.
rkanimozhi221@gmail.com

[1]Corresponding Author E-mail: ujeyamalar@gmail.com

ABSTRACT: In today's the current power distribution networks, electricity theft poses challenges to power reliability and creates significantly large amounts of economic losses. With the implementation of smart meters and the widespread installation of Internet of Things devices, it is necessary to utilize intelligent monitoring strategies for the purpose of detecting abnormal energy usage in real-time. This paper discusses an Intelligent Power Monitoring and Electricity Theft Detection System utilizing the Random Forest machine learning algorithm. RMS feature extraction produces a large amount of data, which is then classified into normal or abnormal electricity consumption patterns using a Random Forest classifier. The Random Forest algorithm is an ensemble classifier that provides accurate classification of the data without overfitting and with low false-positive detection rates. The system communicates in real-time via an IoT communication framework and initiates control once theft detection occurs.

Keywords: Electricity Theft Detection, Intelligent Power Monitoring, Random Forest, RMS Feature Extraction, Internet of Things (IOT), Smart Grid, Real-Time Monitoring, Edge Computing.

1. Introduction

Electricity theft is a major challenge in modern Smart Grids, causing significant financial losses. The 2024 study, "electricity theft detection for smart homes," focuses on identifying these thefts using Machine Learning. By analyzing both real and synthetic (simulated) attack patterns, the research demonstrates how models like Random Forest can accurately detect abnormal energy consumption. This approach ensures that even sophisticated tampering in smart home environments can be identified, providing a robust solution for securing energy data and reducing power losses.

The rapid evolution of smart grids, traditional detection methods are being replaced by more advanced, time-sensitive models. This 2025 study introduces a Hybrid KNN–LSTM framework designed to identify electricity theft with high precision. By combining K-Nearest Neighbors (KNN) for data clustering and Long Short-Term Memory (LSTM) for analyzing time-series consumption patterns, the model effectively captures suspicious behaviors over time. Tested on the industry-standard SGCC (State Grid Corporation of China) dataset, this hybrid approach sets a new performance baseline, proving that integrating spatial and temporal

features is the most effective way to secure modern energy networks.

Smart meter data often contains a lot of noise and a high imbalance between honest users and thieves. solves these problems using a two-step approach: first, it uses Stacked Autoencoders to clean and extract key features from the data. Then, it applies a specialized Random Forest algorithm (UaRe-RF) that uses Under sampling and Resampling to handle imbalanced datasets. This ensures that the model can accurately detect rare theft patterns that would otherwise be missed by standard algorithms.

2. Literature Review

This paper addresses the challenge of highly imbalanced electricity theft data obtained from smart meters. A stacked autoencoder (SAE) is employed to eliminate noise and extract high-level features from raw consumption data. To further improve classification performance, an under sampling and resampling-based Random Forest (UaRe-RF) algorithm is proposed, which balances minority theft samples during training. The results demonstrate improved accuracy and recall compared to traditional machine learning classifiers.[1]

The authors investigate electricity theft detection in smart home environments using both real and synthetically generated attack data. Several machine learning models, including Random Forest, are evaluated under practical residential scenarios. The study shows that Random Forest provides reliable performance and generalization when exposed to different types of theft attacks, making it suitable for real-world deployment. [2]

This work proposes a hybrid framework combining KNN for similarity analysis and LSTM for capturing temporal consumption patterns. Experiments conducted on the SGCC smart-meter dataset indicate high detection accuracy. However, the use of deep learning models results in increased computational complexity and latency, which limits its applicability for edge-based real-time systems.[3] An active learning-based Random Forest model is introduced to reduce the dependency on large labeled datasets. By iteratively selecting the most informative samples for training, the approach enhances detection accuracy while minimizing annotation effort. This method demonstrates the effectiveness of Random Forest when combined with intelligent data selection strategies.[4]

This paper applies Particle Swarm Optimization (PSO) for optimal feature selection and an attention-based LSTM network for abnormal electricity consumption detection. Although the model achieves high accuracy, it requires significant computational resources, making it less suitable for low-power IoT-based monitoring systems. [5]

“Electricity Theft Detection for Smart Homes: Harnessing the Power of Machine Learning with Real and Synthetic Attacks,” the authors propose a machine learning-driven framework for identifying electricity theft in residential smart home environments. The study integrates both real-world smart meter consumption data and synthetically generated theft scenarios to comprehensively evaluate model robustness against diverse attack patterns. Various classifiers are analysed with Random Forest demonstrating consistent performance in terms of accuracy, precision, and generalization capability. Experimental results validate the effectiveness of the proposed approach under practical residential conditions, highlighting its suitability for real-time smart grid monitoring and deployment.[6]

3. Methodology

The proposed methodology is engineered as a multi-layered framework that integrates hardware sensing, intelligent data processing, and automated response. The system architecture is divided into four functional stages: Data Acquisition, Pre-processing, Random Forest Classification, and IoT-based Communication.

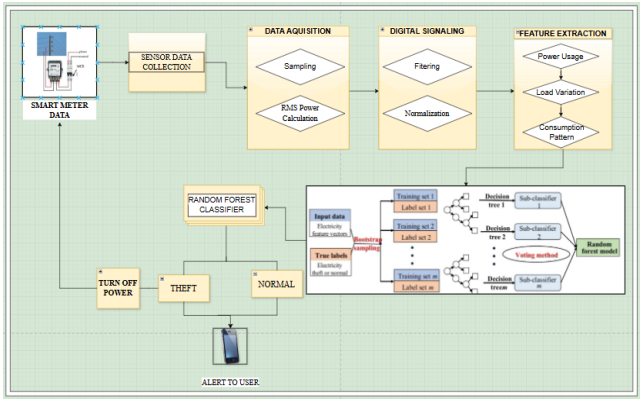

Figure 1: *Block Diagram*

3.1 Data Acquisition and Sensing Layer

In line with the hardware requirements for smart metering, this study adopts a high-precision sensing suite. The physical layer comprises an ESP32 microcontroller, selected for its dual-core processing capability and integrated Wi-Fi stack. To monitor electrical parameters, a ZMPT101B voltage sensor and an ACS712 current sensor are interfaced with the ESP32's analog-to-digital converter (ADC) pins.

The study collects raw waveform data at a high sampling frequency, as suggested in [5], to capture non-linearities and transient spikes that often characterize illegal bypass attempts. The system performs on-chip calculations to transform raw instantaneous values into Root Mean Square (RMS) values. This initial feature set provides the baseline for power consumption patterns, power factor analysis, and load profiling.

3.2 Pre-processing and Feature Extraction

Raw energy data in distribution networks is inherently noisy and often exhibits a significant "class imbalance"—where normal consumption instances vastly outnumber theft instances. Following the logic in [1], a Stacked Autoencoder (SAE) approach is utilized for feature extraction. The SAE functions by compressing the input data into a lower-dimensional latent space and then reconstructing it; the features learned during this process are more robust against sensor noise than raw RMS values.

To solve the "Needle in a Haystack" problem associated with rare theft events, this study implements a hybrid Under sampling and Resampling technique. This ensures that the dataset contains a balanced ratio of "Normal" and "Theft" labels, preventing the machine learning model from developing a bias toward the majority class.

3.3 Random Forest Classification Logic

The core of the detection engine is the Random Forest (RF) ensemble. Unlike individual decision trees that are prone to overfitting, the RF model constructs a multitude of decision trees during training.

Tree Branching: Each tree in the forest is trained on a random subset of data. Inspired by the active learning approach in [4], the branching logic evaluates the correlation between sudden current drops and voltage stability. This allows the system to differentiate between a heavy appliance being turned off (normal) and a partial meter bypass (theft).

Ensemble Voting: As established in [2], the final classification label is determined via a majority vote across all trees. This collective intelligence significantly reduces False Positives, which are common during high-usage periods like festival seasons or summer peaks.

3.4 IoT Communication and Response Mechanism

Once the Random Forest engine classifies a state as "Theft," the system triggers an immediate response protocol as referenced in [3]. The ESP32 executes a two-fold action:

Local Hardware Isolation: The microcontroller sends a high signal to a 5V Relay Module, which physically disconnects the load from the power line, preventing further unauthorized energy consumption.

Cloud Synchronization: Utilizing the MQTT (Message Queuing Telemetry Transport) protocol, the system publishes the alert, timestamp, and energy logs to a cloud-based dashboard. This creates a transparent, tamper-proof audit trail for utility providers to conduct field inspections.

3.5 State Estimation and Validation

To validate the detection, a State Estimation approach is used to compare the observed load with a predicted baseline. If the deviation exceeds a threshold determined by historical home activity [4], the system confirms the classification. This redundancy ensures that hardware malfunctions are not mislabelled as intentional theft, maintaining the reliability of the provincial power grid monitoring.

4. Result & Discussion

4.1 Experimental Setup

The proposed electricity theft detection system was tested based on the voltage and current information obtained from the ESP32-based smart meter prototype. Both normal and electricity theft conditions were achieved with partial meter bypassing and abnormal load changes, as proposed in the experimental section of Lin et al. [1] and Ahmed et al. [2]. To alleviate class imbalance, undersampling or resampling methods have been used.

4.2 Performance Analysis

The performance of the suggested RF classifier was assessed using measurements such as accuracy, recall, and latency. Table I compares the suggested system to recent machine learning-based theft detection models.

Table 1: *Performance Comparison of Theft Detection Models*

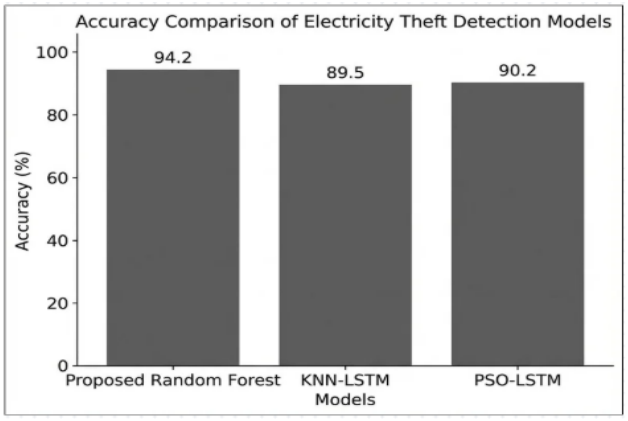

Figure 3: *Accuracy comparison of the preposed random fores*

The proposed system provides higher accuracy than deep learning-based models yet with low latency suitable for real-time operation.

4.3 Discussion

The result shows that using Random Forest classifiers for detecting electricity theft is effective, even with appropriate data balancing. Moreover, the proposed approach has significantly less computation power requirements compared with using LSTM-based detection mechanisms as seen in references [3], [5]. Although using more sophisticated approaches like quantum and graph-based approaches in references [6], [16] has good potential for accurate detection, it is still difficult to implement such approaches..

5. Future Enhancement

The proposed system can also be improved by the incorporation of advanced techniques in machine learning and deep learning, which can enhance the performance and flexibility of the proposed system. Specifically, the incorporation of the Long Short-Term Memory (LSTM) technique can greatly improve the performance of the proposed system in detecting electricity consumption patterns. This is because the data related to the power consumption is sequential and time-dependent in nature. The use of the LSTM model can greatly improve the performance of the proposed system in detecting electricity consumption patterns. This is because

the proposed system can use the proposed technique in detecting any unusual patterns in the data.

In addition, the integration of adaptive feature selection methods can assist the system in identifying the parameters that are of most importance in the energy consumption process. By selecting the most important features, the complexity of the system can be reduced, thereby increasing the detection performance. Besides, there are optimization techniques, including hyperparameter optimization, regularization, and automated retraining, which can improve the robustness of the detection model, particularly in response to changes in load conditions. This is significant since, in most cases, consumers' patterns change, particularly during certain seasons or because of their lifestyles or industrial needs.

Future implementations may also consider scalable cloud-based and edge computing solutions to address the needs of large-scale deployment. Cloud-based solutions can offer data storage, processing, and analytics to monitor all consumers in real-time. At the same time, edge computing can facilitate real-time anomaly detection to reduce latency and conserve network bandwidth. Furthermore, the inclusion of robust data security features and data privacy solutions, such as data encryption and secure data communication, can improve the reliability of the system and ensure reliable operation in a large-scale smart grid environment.

6. References

1. Guoying Lin; Xiaofeng Feng; Wenchong Guo; Xueyuan Cui; Shengyuan Liu; Weichao Jin; Zhenzhi Lin; Yi Ding, Year: 2021, "Electricity theft detection based on stacked autoencoder and the under sampling and resampling based random forest algorithm", IEEE Access, Vol. 9, pp. 124049–124058.

2. Olufemi Abiodun Abraham; Hideya Ochiai; Md Delwar Hossain; Yuzo Taenaka; Youki Kadobayashi, Year: 2024, "Electricity theft detection for smart homes: Harnessing the power of machine learning with real and synthetic attacks", IEEE Access, Vol.12, pp. 26023–26045.

3. Stephanie Ness, Year: 2025, "Hybrid KNN–LSTM framework for electricity theft detection in smart grids using SGCC smart meter data", IEEE Access, Vol. 13, pp. 191809191823.

4. Sidra Abbas; Imen Bouazzi; Stephen Ojo; Gabriel Avelino Sampedro; Ahmad S. Almadhor; Abdullah Al Hejaili; Zuzana Stolicna, Year: 2024, "Improving Smart Grids Security: An Active Learning Approach for Smart Grid-Based Energy Theft Detection", IEEE Access, vol. 12, pp. 17061717.

5. Jiahao Bian; Lei Wang, Rafał Scherer; Marcin Woźniak; Pengchao Zhang; Wei, Year: 2021, "Abnormal detection of electricity consumption of user based on particle swarm optimization and long short term memory with the attention mechanism", IEEE Access, vol. 9, pp. 47252–47265.

6. Konstantinos Blazakis; Nikolaos Schetakis; Mahmoud M. Badr; Davit Aghamalyan, Konstantinos Stavrakakis; Georgios Stavrakakis, Year: 2025, "Power theft detection in smart grids using quantum machine learning", IEEE Access, vol. 13, pp. 6151161525.