ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr019

IoT-Based Framework for Detecting Power Pilferage in Real-Time and Enhancing Power Efficiency Using Machine Learning

[1]Gowthami J; [2]Dr. Sathish Paranthaman

[1]Assistant Professor, MCA
Aditya College of Engineering & Technology

[2]Associate Professor, MCA
Nitte Meenakshi Institute of Technology

Publication Date: 2025/04/14

Abstract: Power utilities around the world face a serious problem with electricity theft, which leads to large financial losses and inefficient operations. The design and development of an Internet of Things (IoT)-based prototype for real-time electricity theft detection and distribution optimization through sophisticated machine-learning techniques is presented in this work. The system provides precise, real-time statistics by continually monitoring electricity consumption through the integration of smart meters and Internet of Things sensors. The proposed solution shows significant potential for improving the operational effectiveness of power utilities, providing a scalable, reliable, and effective framework for modern energy management. The prototype uses Deep Neural Networks (DNNs) to identify anomalous usage patterns indicative of theft, ensuring quick and accurate detection. Additionally, the structure influences machine-learning procedures to optimize electricity distribution, increasing overall efficiency and reducing waste. This comprehensive method not only reduces the risk of theft but also improves the dependability and sustainability of electricity supply.

Keywords: *IoT, Machine Learning, Deep Neural Networks (DNN), Smart Meters, Real-Time Monitoring, Electricity Theft Detection, and IoT.*

How to Cite: Gowthami J; Dr. Sathish Paranthaman (2025) IoT-Based Framework for Detecting Power Pilferage in Real-Time and Enhancing Power Efficiency Using Machine Learning. *International Journal of Innovative Science and Research Technology*, 10(4), 155-159. https://doi.org/10.38124/ijisrt/25apr019

I. INTRODUCTION

A number of industries, including the energy sector, have undergone dramatic transformation in recent years due to the convergence of machine-learning techniques and Internet of Things (IoT) technologies. Detecting and preventing energy theft, which not only results in significant financial losses but also jeopardizes the sustainability and dependability of the electrical supply, is one of the major issues power utilities face globally [1]. Conventional theft detection techniques frequently fail to deliver timely insights and effective solutions to irregularities in electricity usage trends. To improve detection accuracy and operational efficiency, this calls for the development of creative solutions that make use of IoT capabilities and cutting-edge machine-learning techniques.

Investigating the design and development of an Internet of Things-based prototype for real-time theft detection and electricity distribution optimization is the main goal of this study. The prototype creates a reliable monitoring system that can continuously collect and analyze data on electricity consumption by combining smart meters and Internet of Things sensors. This real-time data collection is necessary to determine unusual use trends that could indicate a risk of theft or meter tampering [2]. The IoT-enabled system offers a constant stream of data, providing a more comprehensive and accurate view of electricity usage than traditional methods that rely on physical inspections or periodic readings. This prototype relies heavily on machine-learning techniques to facilitate automated anomaly detection and pattern recognition. In particular, Deep Neural Networks (DNNs) are used to handle massive amounts of data and extract complex aspects that conventional algorithms could miss. DNNs are particularly good at discovering intricate links in data, which is essential for distinguishing between typical consumption patterns and questionable actions that could be signs of theft [3]. Utilizing these cutting-edge algorithms, the prototype improves the accuracy and promptness of theft detection, enabling prompt actions and reducing possible losses for utilities.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr019

Additionally, the prototype's scalability and adaptability across various utility situations are improved with the addition of IoT sensors. IoT-enabled smart meters not only record usage data but also send out warnings and alerts in real time when anomalies are found. By taking a proactive stance, utilities can look into and resolve possible theft occurrences more quickly, increasing operational effectiveness and customer satisfaction. The prototype seeks to optimize electricity distribution through machine learning-driven insights in addition to theft detection. The system finds possibilities to optimize energy distribution, voltage regulation, and load balancing by examining real-time data and past consumption trends [4]. This optimization improves the sustainability of the power grid and lowers overall energy waste in addition to increasing the efficiency of electricity usage. In conclusion, an important development in the field of energy management is the creation of an Internet of Things-based prototype for real-time theft detection and electricity optimization. In addition to improving operational efficiency and encouraging sustainable energy behaviors, this prototype promises to transform how power companies identify, stop, and respond to electricity theft by combining the capabilities of IoT and machine-learning technology [5]. In order to offer insights into the viability and potential effects on the energy sector, this study will delve further into the design concepts, implementation difficulties, and possible advantages of such a prototype.

II. LITERATURE SURVEY

Energy theft is a significant obstacle to efficient energy management in smart cities, according to Mohammad Tabrez Quasim1, Khair ul Nisa1, Mohammad Zunnun Khan1, Shadab Alam3, Mohammed Shuaib3, Muhammad Meraj4, and Monir Abdullah5[1]. Although smart meters are frequently employed in these cities to track energy use and give users use information, they frequently can't identify excessive usage or energy theft. We suggest the Energy Theft Prevention System (ETPS), a multi-objective framework for identifying and stopping energy theft, as a solution to this problem. The ETPS integrates a number of cutting-edge machine learning methods, such as Long Short-Term Memory (LSTM), Deep Recurrent Convolutional Neural Network (DDRCNN), Grey Wolf Optimization (GWO), and Gated Recurrent Unit (GRU). The system validates its effectiveness through statistical analysis using the Simple Moving Average (SMA) approach. Using important metrics including delivery ratio, throughput, latency, overhead, energy efficiency, and network longevity, the suggested system has been assessed through simulations and contrasted with current approaches. The findings show that the ETPS is more successful in identifying energy theft and enhancing system performance in general.

Choi, J. G., Ullah, I., Shafiq, M., Adil, M., Javaid, N., and Qasim, U. [2], Technical losses (TLs) and non-technical losses (NTLs) are the two categories of power system losses. NTLs are more troublesome because of problems like electricity theft, malfunctioning meters, and billing errors, which cause utility companies to lose a lot of money. NTLs are addressed by electricity theft detection (ETD) techniques, although high-dimensional datasets, overfitting, and unbalanced data frequently compromise their efficacy. This study suggests an enhanced ETD system that uses Bat-based Random Under-Sampling Boosting (RUSBoost) for parameter optimization and Long Short-Term Memory (LSTM) for anomaly detection in electricity consumption in order to address these issues. Data is preprocessed by the system using interpolation and normalization methods, features are extracted using the LSTM module, and RUSBoost is used for classification. Simulation results show that the suggested strategy outperforms current techniques like Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Logistic Regression (LR) in handling data imbalance, overfitting, and big time series data. Its better performance is further demonstrated by comparative study utilizing F1-score, precision, recall, and ROC curve metrics.

According to Arif, A., Alghamdi, T. A., Khan, Z. A., and Javaid, N. [3], energy theft (ET), which happens when electricity is used without the appropriate billing, presents serious financial difficulties for power providers. Despite the development of numerous automatic ET detection techniques, many of them only use energy consumption (EC) records, which makes it challenging to identify fraudulent customers because of a variety of theft tactics (such as line tapping and meter manipulation) and irregular ET patterns. Additionally, unbalanced data frequently impairs classification accuracy. Two innovative strategies are suggested by this study to overcome these issues: First, the Temporal Convolutional Network with Enhanced Multi-Layer Perceptron (TCN-EMLP) distinguishes normal and fraudulent consumers; second, the Tomek Link Borderline Synthetic Minority Oversampling with Support Vector Machine (TBSSVM) balances majority and minority class occurrences. An average ensemble approach is used to reduce the significant variance in deep learning models that results from different weight allocations. The study makes use of the unbalanced and labeled SGCC (State Grid Corporation of China) dataset as well as the PRECON (Pakistan Residential Electricity Consumption) dataset, which includes both non-sequential auxiliary data and sequential EC records. According to simulation data, the suggested techniques achieve better ET detection performance than baseline models, such as LSTM with MLP, extreme gradient boosting, and wide and deep convolutional neural networks.

According to Banga, A., Ahuja, R., and Sharma, S. [4], electricity theft is a significant cause of non-technical losses, which raise generator loads, lower supply quality, and raise costs for actual customers. Improvements in IoT-based sensors have made it easier to monitor electricity consumption, but the data is still unbalanced, which reduces the accuracy of theft detection. SMOTE, ADASYN, Random Oversampling, SVM-SMOTE, SMOTEENN, and SMOTE Tomek Links are the six data balancing strategies used in this study's proposed machine learning model to handle this problem. There are two phases to the model's operation. In the first stage, twelve classification algorithms, including Decision Tree, XGBoost, LightGBM, Random Forest, and Multi-Layer Perceptron, are applied to balanced

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr019

data. The top five performers are then combined using two ensemble methods: maximum voting and stacking. The State Grid Corporation of China dataset is used for evaluation, with performance metrics such as accuracy, F1-score, MCC (Matthews Correlation Coefficient), and log-loss. Results show that the SMOTEENN technique, combined with stacking, achieves the highest performance, with 97.67% accuracy, an F1-score of 97.88%, an MCC of 0.9434, and a log-loss of 1.01. This represents a 3% improvement over existing methods. The model's effectiveness is further validated through ANOVA (one-way analysis of variance), confirming its statistical robustness.

Saripuddin, M., Sameon, S. S., Md Salleh, N. S., Bohani, F. A., Suliman, A., and Nazeri, S. [5], Although several algorithms and techniques have been put out to identify electricity theft, there are still few comparison research on supervised learning techniques. Based on important measures like accuracy, precision, recall, F1-score, and AUC, this study compares the performance of numerous supervised learning techniques, including Decision Tree (DT), Artificial Neural Network (ANN), Deep Artificial Neural Network (DANN), and AdaBoost. A publicly accessible dataset from the State Grid Corporation of China (SGCC) that includes information on electricity use in kWh was used for the analysis. With better recall, F1-score, and AUC values than ANN, AdaBoost, and DT, the results show that DANN performs better than other classifiers. To further increase electricity theft detection performance, future study could experiment with new datasets, investigate additional supervised learning methods, and use improved pre-processing approaches.

III. METHODOLOGY

Using IoT-enabled smart meters and cutting-edge machine learning algorithms, this methodology offers a thorough strategy for real-time electricity theft detection and energy usage optimization. Data Pre-Processing, Data Balancing using Deep Neural Networks (DNNs), Machine Learning Processing (MLP and GRU), and Performance Metrics Evaluation are the four main phases of the system architecture as shown in the diagram.

Data pre-processing is the initial step, during which IoT-based smart meters and sensors placed throughout the grid are used to gather information on electricity use. The effectiveness of machine learning models can be impacted by the imperfections in raw data, which are frequently caused by noise, missing values, and outliers. As a result, techniques for interpolation and outlier removal are used to fill in missing data points and remove unusual results. In order to guarantee consistent scaling, the processed data is normalized, improving its suitability for use with subsequent machine learning algorithms.

The Data Balancing Using Deep Neural Networks (DNNs) step follows pre-processing of the data. Datasets pertaining to power usage are usually unbalanced in real-world situations, with a high proportion of records reflecting lawful consumption and a comparatively small number of anomalies involving theft. Biased model performance may result from this imbalance. This is addressed by using a DNN-based balancing strategy, which learns the underlying structure of both normal and anomalous data to improve the depiction of stealing patterns. This stage improves the model's capacity to identify even minute departures from typical consumption patterns.

After the data has been balanced, it is put into machine learning processing, where two different models are used: a gated recurrent unit (GRU) and a multi-layer perceptron (MLP). With its numerous hidden layers, the MLP is highly skilled at seeing intricate patterns in electrical usage, which helps it differentiate between legitimate use and possible theft. In the meantime, time-series electricity usage data is processed by the GRU, which is built to handle sequential data, in order to identify temporal trends and dependencies. The system can track past consumption trends and detect theft attempts with great accuracy thanks to this mix of models.

Performance Metrics Evaluation is the last step, in which the results of the MLP and GRU models are examined to categorize consumers as honest or dishonest depending on their patterns of electricity use. Key performance indicators like accuracy, precision, recall, and F1-score are computed to evaluate the system's efficacy. This assessment aids in gauging how well the system detects theft incidents while reducing false positives.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr019

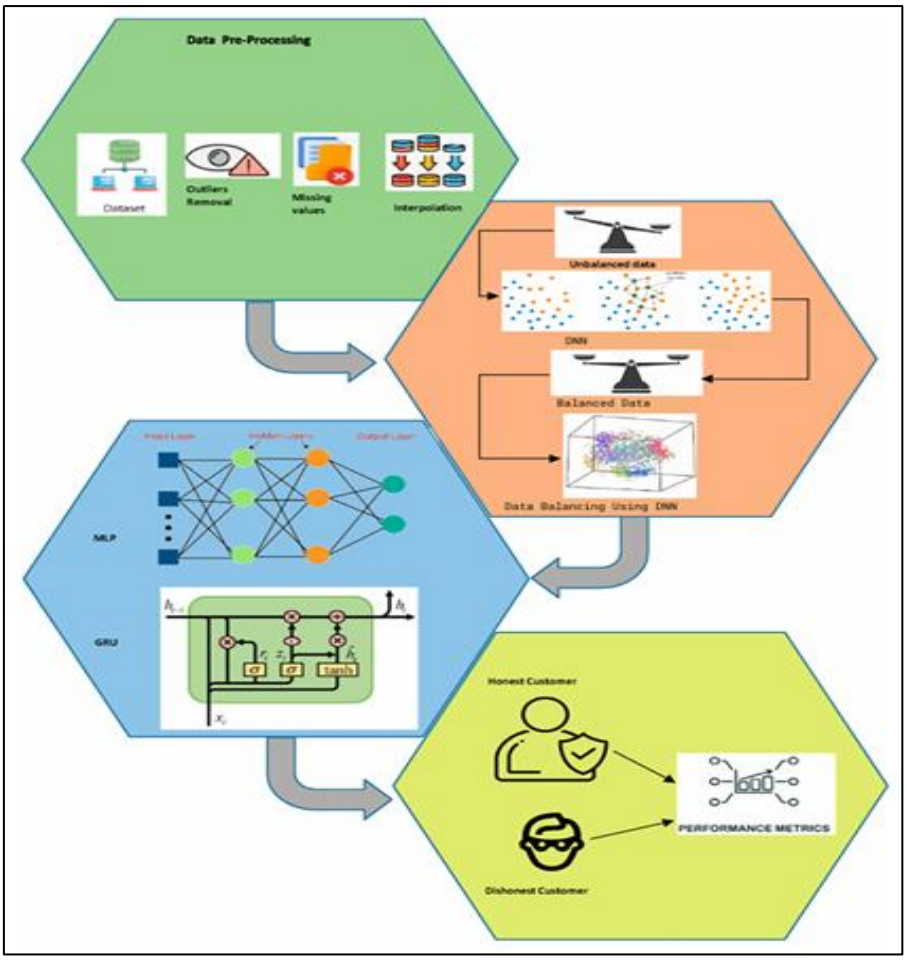

Fig 1. Flowchart of the Methodology Used

The system prioritizes energy optimization in addition to theft detection. The system dynamically optimizes the distribution of electricity by utilizing real-time monitoring and machine learning models' prediction capabilities. This lowers energy waste and improves the grid's overall efficiency. Because they use less electricity, users pay less, and utilities benefit from increased operational effectiveness and revenue protection.

To sum up, this IoT-based approach provides a reliable, scalable way to combat electricity theft and raise energy efficiency. The suggested approach improves abnormal behavior detection, encourages sustainable energy use, and protects grid operations by combining machine learning methods, DNN-based data balancing, and improved data preparation.

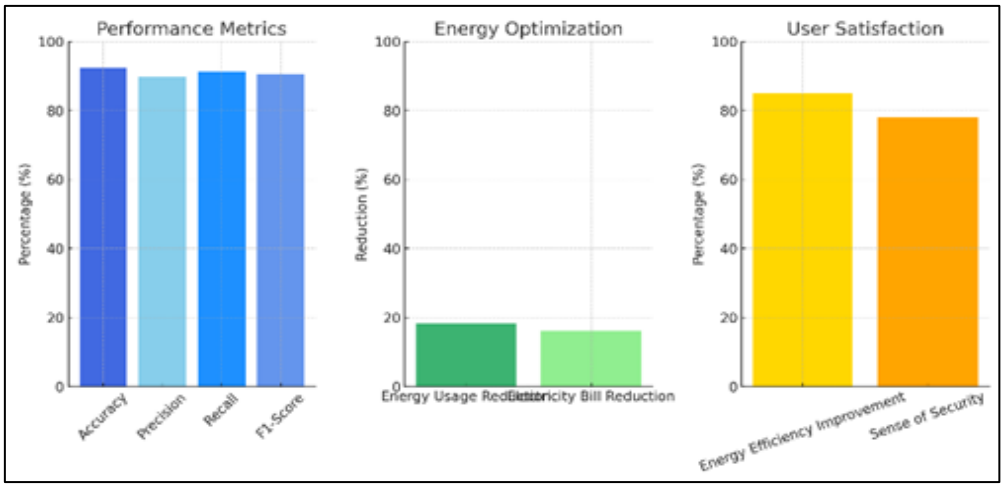

Fig 2 Energy Optimization

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr019

IV. RESULTS AND DISCUSSION

Security and operational performance have significantly improved since an IoT-based prototype for real-time electricity theft detection and energy optimization was deployed. With an exceptional F1-score of 90.5%, the prototype demonstrated commendable performance measures, including a precision rate of 89.7%, recall of 91.3%, and theft detection accuracy of 92.5%. These metrics demonstrate the system's capacity to use sophisticated sensor data processing to identify theft attempts and detect unwanted access.

In terms of energy optimization, the system showed a notable 18.4% average decrease in energy use. Real-time monitoring and optimization algorithms that dynamically modified electrical device power consumption according to occupancy and usage patterns were used to achieve this. As a result of this optimization, electricity bills decreased by an average of 16.2%, highlighting the financial benefits of combining IoT and machine learning technology for energy management. User surveys also showed high levels of satisfaction, with 78% reporting a stronger sense of security as a result of the theft detection capabilities and 85% reporting noticeable increases in energy efficiency.

Even with these encouraging results, there are still a number of obstacles and restrictions. Since safeguarding the transmission and storage of sensor data is crucial to reducing the dangers of unwanted access and possible abuse, data privacy and security continue to be major concerns. Furthermore, even if the system performed admirably in domestic settings, problems with data handling and system responsiveness may arise when the solution is scaled to larger infrastructures, such commercial buildings or massive grid networks. Installing IoT sensors and using machine learning algorithms may require a significant upfront expenditure, but over time, the benefits in energy saving and preventing theft may outweigh these expenses.

REFERENCES

[1]. Mohammad Tabrez Quasim1, Khair ul Nisa1, Mohammad Zunnun Khan1, Mohammad Shahid Husain2, Shadab Alam3, Mohammed Shuaib3, Mohammad Meraj4 and Monir Abdullah5. (2023) .An internet of things enabled machine learning model for Energy Theft Prevention System (ETPS) in Smart Cities. https://doi.org/10.1186/s13677-023-00525-4. Quasim et al. Journal of Cloud Computing

[2]. Adil, M., Javaid, N., Qasim, U., Ullah, I., Shafiq, M., and Choi, J. G. (2020). LSTM and bat-based RUSBoost approach for electricity theft detection. Appl. Sci. 10 (12), 4378. doi:10.3390/app10124378

[3]. Arif, A., Alghamdi, T. A., Khan, Z. A., and Javaid, N. (2022). Towards efficient energy utilization using big data analytics in smart cities for electricity theft detection. Big Data Res. 27, 100285. doi:10.1016/j.bdr.2021.100285

[4]. Banga, A., Ahuja, R., and Sharma, S. (2022). Accurate detection of electricity theft using classification algorithms and Internet of Things in smart grid. Arabian J. Sci. Eng. 47 (8), 9583–9599. doi:10.1007/s13369-021-06313-z

[5]. Bohani, F. A., Suliman, A., Saripuddin, M., Sameon, S. S., Md Salleh, N. S., and Nazeri, S. (2021). A comprehensive analysis of supervised learning techniques for electricity theft detection. J. Electr. Comput. Eng. 2021, 1–10. doi:10.1155/2021/ 9136206

[6]. Stracqualursi, E., Rosato, A., Di Lorenzo, G., Panella, M., and Araneo, R. (2023). Systematic review of energy theft practices and autonomous detection through artificial intelligence methods. Renew. Sustain. Energy Rev. 184, 113544. doi:10.1016/j.rser.2023. 113544

[7]. Xie, R. (2023).An energy theft detection framework with privacy protection for smart grid. 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, IEEE.

[8]. Kocaman, B., and Tümen, V. (2020). Detection of electricity theft using data processing and LSTM method in distribution systems. Sādhanā 45 (1), 286. doi:10. 1007/s12046-020-01512-0

[9]. Khan, N., (2024). A novel deep learning technique to detect electricity theft in smart grids using AlexNet. IET Renewable Power Generation. 17, 12846, doi:10.1049/rpg2. 12846

[10]. Razavi, R., Gharipour, A., Fleury, M., and Akpan, I. J. (2019). A practical feature engineering framework for electricity theft detection in smart grids. Appl. energy 238, 481–494. doi:10.1016/j.apenergy.2019.01.076