Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

An Intelligent AI-Driven Framework For Electricity Theft Detection In Smart Grid Systems

Grishma Mhaske, Sakshi Shinde, Atharv Balve, Prof. N. A. Pondhe
Department of Computer Science & Design
Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar

Abstract - **Electricity theft is a major challenge faced by power distribution companies worldwide, leading to significant financial losses, reduced grid reliability, and increased safety risks. With the rapid deployment of smart grids and advanced metering infrastructure, large volumes of electricity consumption data are generated at regular intervals. Traditional theft detection methods based on manual inspection and rule-based analysis are inefficient, time-consuming, and incapable of identifying complex and concealed theft patterns. To overcome these limitations, this project proposes an Artificial Intelligence (AI)–based approach for detecting electricity theft by analyzing consumer energy usage behavior using smart meter data.**

The proposed system employs an Artificial Neural Network (ANN) model trained on historical electricity consumption data to identify abnormal patterns indicative of theft. Key statistical features such as mean, median, maximum, minimum, standard deviation, sum of energy consumption, and record count are extracted after thorough data preprocessing. The trained ANN model demonstrates high accuracy in distinguishing between normal and suspicious consumption behavior. A Flask-based web application is developed to provide a user-friendly interface for real-time prediction and visualization of results. This intelligent and scalable solution enhances grid security, minimizes non-technical losses, and supports efficient decision-making for utility providers, while also offering potential applicability in other anomaly detection domains.

Keywords - Electricity Theft, Smart Grids, Artificial Neural Network (ANN), Machine Learning, Anomaly Detection, Energy Consumption Analysis, Smart Meter Data, AI-Based Detection, Flask Web Application, Utility Security

I. INTRODUCTION

Electricity has become a fundamental necessity for modern society, supporting residential living, industrial production, healthcare services, and digital infrastructure. With the rapid increase in population and urbanization, the demand for electrical energy has grown significantly. Power utilities across the world face the dual challenge of meeting rising demand while maintaining efficiency and reliability in electricity distribution systems. Among the various challenges, electricity theft remains one of the most critical issues, causing substantial economic losses and operational inefficiencies for power distribution companies [1].

Electricity theft is classified as a non-technical loss (NTL) and includes activities such as meter tampering, illegal connections, bypassing meters, and manipulating billing systems. These practices not only result in revenue loss but also degrade the quality of power supply and increase operational costs. In many developing countries, electricity theft contributes to a large percentage of total power losses, forcing utilities to increase tariffs for honest consumers and creating social and economic imbalance [2]. Additionally, illegal power usage poses severe safety risks, including fire hazards, equipment damage, and threats to human life [3].

Traditional approaches for detecting electricity theft rely heavily on manual inspections, customer complaints, and periodic audits. These methods are labor-intensive, time-consuming, and often ineffective in identifying sophisticated theft techniques. Moreover, manual inspections are prone to human error, corruption, and limited coverage, especially in densely populated or remote areas. Rule-based detection systems, which flag abnormal consumption based on predefined thresholds, also suffer from high false-positive rates and lack adaptability to changing consumption behaviors [4].

The emergence of smart grids has transformed conventional power distribution networks into intelligent, data-driven systems. Smart grids integrate advanced sensing, communication, and control technologies that enable real-time monitoring of electricity consumption. Smart meters, a core component of smart grids, record high-resolution consumption data at regular intervals and transmit it to utility servers through Advanced Metering Infrastructure (AMI) [5]. This continuous data generation provides an opportunity to analyze consumer behavior in greater detail than ever before.

However, the massive volume, velocity, and variety of smart meter data make manual analysis impractical. Extracting meaningful insights from such large datasets requires advanced computational techniques capable of identifying hidden patterns and anomalies. This challenge has led to the increasing adoption of Artificial Intelligence (AI) and Machine Learning (ML)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

techniques in power systems for tasks such as load forecasting, fault detection, and energy theft identification [6][7].

Artificial Neural Networks (ANNs), inspired by the structure and functioning of the human brain, have shown exceptional performance in pattern recognition and classification problems. ANNs are capable of learning complex, nonlinear relationships from data, making them well-suited for detecting subtle and concealed electricity theft behaviors. Unlike traditional statistical methods, ANN-based models adapt to evolving consumption patterns and improve their performance with increased data availability [8][9].

Recent research has demonstrated that AI-based theft detection systems significantly outperform conventional methods in terms of accuracy and reliability. By analyzing historical consumption data and extracting statistical features such as mean, variance, peak usage, and load irregularities, machine learning models can effectively distinguish between legitimate and suspicious usage patterns [10][11]. Deep learning architectures further enhance detection performance by capturing temporal and behavioral patterns in energy consumption data [12].

Despite these advancements, implementing AI-based theft detection systems in real-world environments presents several challenges. Issues such as data imbalance between normal and theft cases, missing or noisy data, and privacy concerns must be carefully addressed. Proper data preprocessing, feature engineering, and model optimization are essential to ensure robust and reliable system performance [13]. Additionally, the interpretability and scalability of AI models remain important considerations for large-scale deployment.

To address these challenges, this project proposes an ANN-based electricity theft detection system using smart grid consumption data. The system focuses on extracting meaningful statistical features from preprocessed data and training an optimized ANN model to classify consumption behavior accurately. By integrating the trained model with a Flask-based web application, the system provides a practical and user-friendly solution for real-time theft detection [14].

In conclusion, the integration of Artificial Intelligence with smart grid infrastructure offers a powerful approach to combating electricity theft. AI-driven systems not only reduce non-technical losses but also enhance grid reliability, operational efficiency, and revenue assurance for utilities. The proposed approach contributes to the growing body of research in intelligent power systems and demonstrates the potential of AI in addressing critical challenges within modern energy networks [15].

II. LITERATURE SURVEY

The study titled Electricity Theft Detection in Smart Grid Using Machine Learning presents an advanced hybrid deep learning framework for identifying electricity theft in smart grid environments. The authors highlight major challenges in traditional detection techniques, including class imbalance, high-dimensional smart meter data, and limited adaptability to evolving theft patterns. To overcome these issues, a hybrid model combining Multi-Layer Perceptron (MLP) and Gated Recurrent Unit (GRU) networks is proposed and trained on real smart meter data collected from the Chinese National Grid Corporation. Comprehensive data preprocessing techniques such as normalization, missing value handling, and k-means SMOTE are employed to enhance data quality and balance the dataset. The hybrid MLP-GRU model effectively captures both consumption behavior trends and temporal dependencies, resulting in superior performance compared to existing deep learning models. Experimental results demonstrate improved accuracy, precision, recall, and robustness, confirming the effectiveness of hybrid deep learning approaches for real-world electricity theft detection in smart grids [1].

A novel electricity theft detection approach based on Deep Reinforcement Learning is introduced to address the limitations of traditional supervised learning models in adapting to dynamic power consumption behavior and emerging cyber-attacks. The proposed framework utilizes Deep Q-Network and Double Deep Q-Network architectures, allowing the detection model to continuously learn optimal decision-making policies through interaction with the smart grid environment. Unlike static classifiers, the reinforcement learning agent dynamically adapts to changes such as new customer onboarding, fluctuating energy usage patterns, and zero-day attacks. Experimental evaluations conducted under multiple real-world scenarios demonstrate that DRL-based models achieve higher detection accuracy and better adaptability compared to conventional deep learning techniques. This study highlights the strong potential of reinforcement learning for real-time, adaptive, and intelligent electricity theft detection in modern smart power grids [2].

A real-time electricity theft detection framework using supervised machine learning techniques is proposed to overcome the inefficiencies of traditional inspection-based detection systems. The approach employs Support Vector Machine and XGBoost algorithms to analyze smart meter data streams and identify fraudulent consumption patterns. The system is evaluated using synthetic datasets that closely resemble real-world consumer behavior, including both normal and theft scenarios. Comparative analysis shows that XGBoost outperforms SVM by effectively handling nonlinear and complex consumption patterns while maintaining higher accuracy and lower false positives. The study also discusses practical deployment challenges such as computational overhead, data privacy concerns, and system scalability. The findings confirm that machine learning-based real-time detection systems offer efficient and cost-effective solutions for reducing non-technical losses in smart grid environments [3].

A robust data-driven electricity theft detection framework is presented using an improved Artificial Neural Network

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

architecture designed to enhance system reliability and attack resilience. The proposed method addresses common issues in smart meter data, including missing values, outliers, high variance, and data imbalance, through a structured preprocessing and hybrid resampling strategy. The improved ANN model integrates regularization techniques, optimized hyperparameter selection, and skip connections to mitigate overfitting and improve generalization capability. Experimental validation on real-world datasets demonstrates that the proposed framework achieves superior accuracy, stability, and consistency compared to traditional machine learning and deep learning approaches. The results indicate that optimized ANN-based models are highly suitable for large-scale and attack-resilient electricity theft detection systems [4].

An AI-enabled electricity theft detection model is proposed that combines time-domain and frequency-domain feature analysis to improve classification accuracy in smart grids. The framework utilizes deep neural networks trained on smart meter data obtained from the State Grid Corporation of China to capture complex consumption patterns. By incorporating frequency-domain features alongside temporal data, the model enhances its ability to distinguish between normal and fraudulent behavior. Bayesian optimization is applied to fine-tune critical hyperparameters such as network depth and activation functions, leading to reduced false alarms and improved detection efficiency. Experimental results validate the effectiveness of the proposed approach for real-time smart grid monitoring and electricity theft detection, demonstrating the advantages of AI-driven methods in modern power systems [5].

III. PROPOSED SYSTEM

A. System Architecture and Data Flow

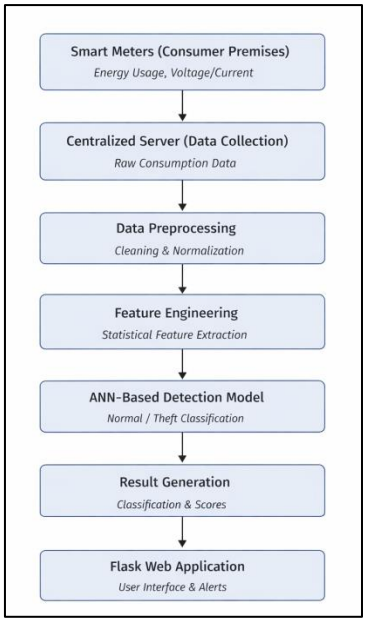


Fig 1: Proposed System

The proposed system is designed as an intelligent, data-driven framework for detecting electricity theft in smart grid environments by leveraging Artificial Intelligence techniques. The architecture begins with the integration of smart meters deployed at consumer premises, which continuously record electricity consumption and related electrical parameters at fixed time intervals. These smart meters form part of the Advanced Metering Infrastructure (AMI) and act as the primary data source for the system. The collected data is securely transmitted to a centralized server, where it is stored and prepared for further analysis. This centralized approach enables utilities to monitor a large number of consumers simultaneously and provides a scalable solution for theft detection across extensive power distribution networks.

Once the raw consumption data is collected, it is passed through a preprocessing layer that ensures data reliability and consistency. This stage handles missing values, eliminates noise, and normalizes consumption records to a uniform scale. Preprocessing is essential because smart meter data often contains irregularities due to communication failures, sensor errors, or incomplete readings. After cleaning, the data is transformed into meaningful statistical representations through feature extraction. Key features such as mean energy consumption, median usage, maximum and minimum values, standard deviation, total energy usage, and record count are computed. These features compactly represent consumer behavior patterns and help differentiate between normal and abnormal consumption trends.

The extracted features are then fed into the Artificial Neural Network (ANN)–based detection engine. The ANN model is trained using historical labeled data that includes both legitimate and theft-related consumption patterns. Through multiple hidden layers and nonlinear activation functions, the ANN learns complex relationships within the data and identifies subtle anomalies that are difficult to detect using traditional rule-based methods. The trained model outputs a classification indicating whether the given consumption pattern is normal or suspicious. Finally, the results are displayed through a Flask-based web application, allowing utility operators to view predictions, monitor suspicious users, and take timely action. This architecture ensures an end-to-end automated workflow from data acquisition to theft detection and visualization.

B. ANN-Based Detection and Web Application Integration

The core intelligence of the proposed system lies in the Artificial Neural Network–based detection model, which is designed to accurately identify electricity theft by analyzing consumption behavior. The ANN consists of an input layer that receives extracted statistical features, multiple hidden layers that perform nonlinear transformations, and an output layer that produces the final classification result. During training, the model adjusts its weights using backpropagation and optimization techniques to minimize prediction error. This

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

learning process enables the ANN to distinguish between normal variations in electricity usage and patterns that indicate possible theft, even when the differences are subtle or intentionally concealed.

To enhance practical usability, the trained ANN model is integrated into a Flask-based web application that serves as the system's user interface. The web application allows authorized users to input new consumption data either manually or through file uploads and receive instant theft detection results. The interface displays the prediction outcome along with confidence levels, making it easier for utility personnel to interpret results without requiring technical expertise in machine learning. This real-time interaction supports quick decision-making and reduces dependency on manual inspections.

The proposed system is designed with scalability and adaptability in mind. As new consumption data becomes available, the model can be retrained or updated to adapt to evolving theft strategies and changing consumer behavior. The modular design of the system allows it to be extended to other anomaly detection applications, such as fraud detection or network intrusion monitoring. By combining intelligent data analysis with a user-friendly deployment platform, the proposed system offers a reliable, efficient, and practical solution for reducing non-technical losses and enhancing the overall security of smart grid infrastructure.

C. Data Preprocessing and Feature Engineering

Data preprocessing plays a critical role in the effectiveness of the proposed electricity theft detection system. Smart meter data collected from real-world environments often contains missing values, inconsistent readings, noise, and class imbalance between normal and theft cases. If such raw data is directly fed into the learning model, it can significantly degrade detection accuracy. To address this issue, the proposed system incorporates a dedicated preprocessing stage that ensures the reliability and consistency of input data before model training and prediction.

In this stage, missing or incomplete values are handled using suitable interpolation and imputation techniques to maintain continuity in consumption records. Noise and extreme outliers caused by faulty meters or communication errors are identified and minimized to avoid misleading the learning process. The data is then normalized to a common scale, which helps the ANN model converge faster and improves stability during training. Since electricity theft cases are usually far fewer than normal cases, data balancing techniques are applied to reduce class imbalance and ensure that the model does not become biased toward normal consumption patterns. This preprocessing framework significantly improves the robustness and generalization capability of the proposed system.

D. Model Training, Validation, and Performance Evaluation

The training and validation phase focuses on building a reliable and accurate ANN model for electricity theft detection. The preprocessed dataset is divided into training and testing sets to evaluate the model's learning capability and generalization performance. During training, the ANN learns the underlying relationships between extracted features and consumption behavior labels by adjusting weights through backpropagation. Activation functions and optimization algorithms are selected to efficiently minimize loss and improve classification accuracy.

Model performance is evaluated using standard metrics such as accuracy, precision, recall, and F1-score to assess detection reliability. High accuracy ensures correct identification of theft cases, while precision and recall help evaluate false alarm rates and missed detections. Validation results demonstrate that the ANN model effectively differentiates between normal and abnormal electricity consumption patterns. Continuous monitoring of these performance metrics allows fine-tuning of model parameters, leading to improved detection capability and reduced false positives, which is essential for real-world deployment in power distribution systems.

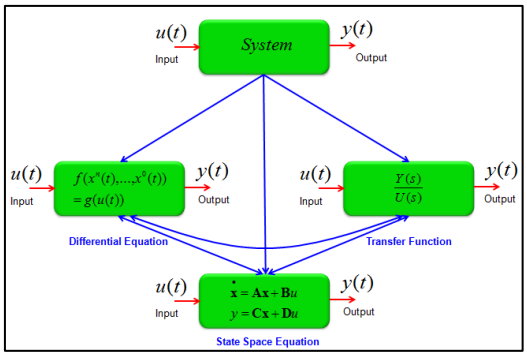
E. System Scalability, Security, and Practical Deployment

The proposed system is designed to support large-scale deployment across smart grid infrastructures with thousands of consumers. Its modular architecture allows seamless integration with existing utility systems and supports expansion as the number of smart meters increases. The centralized processing framework enables efficient handling of high-volume data streams while maintaining consistent detection performance. As consumption behavior evolves over time, the system can be periodically retrained using updated datasets, ensuring adaptability to new theft techniques and changing usage patterns.

From a security perspective, the system ensures that sensitive consumption data is accessed only by authorized users through controlled interfaces. The Flask-based web application provides role-based access and secure communication between users and the server. The practical deployment of the proposed system reduces dependence on manual inspections, lowers operational costs, and enables proactive identification of electricity theft. Overall, the system offers a scalable, secure, and intelligent solution that enhances grid reliability, improves revenue protection, and supports smarter energy management in modern power distribution networks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

IV. MATHEMATICAL MODEL



A. System Overview

The electricity theft detection system is modeled as a classification problem, where smart meter consumption data is analyzed to determine whether a consumer's behavior is Normal or Theft. The model processes historical electricity usage data, extracts statistical features, and applies an Artificial Neural Network (ANN) to classify consumption patterns.

B. Input Data Representation

Let the smart meter consumption data for a consumer be represented as a time series:

$$X = \{x1, x2, x3, \dots, xn\}$$

$$(x + a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

Where:

- xi represents electricity consumption at time interval iii
- n is the total number of recorded intervals

C. Feature Extraction Model

From the raw consumption data X
statistical features are extracted to form a feature vector

1. Mean Energy Consumption

$$\mu = n1i = 1\sum nxi$$

2. Maximum Consumption

$$xmax = max(x1, x2, \dots, xn)\ 3$$

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L}\right)$$

3. Minimum Consumption

$$xmin = \min(x1, x2, \dots, xn)$$

4. Standard Deviation

$$\sigma = n1i = 1\sum n(xi - \mu)2\ 5$$

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots, \qquad -\infty < x < \infty$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

D. ANN-Based Classification Model

The Artificial Neural Network receives the feature vector FFF as input.

Weighted Sum at Neuron

$$z = j = 1\sum mwjfj + b$$

Where:

- wj = weight associated with feature fj
- b = bias term
- mmm = number of features

$$\sin\alpha \pm \sin\beta = 2\sin\frac{1}{2}(\alpha \pm \beta)\cos\frac{1}{2}(\alpha \mp \beta)$$

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots, \qquad -\infty < x < \infty$$

G. Theoretical Interpretation

- Normal consumers exhibit stable statistical patterns in electricity usage.
- Theft cases show abrupt changes, abnormal peaks, or irregular consumption.
- The ANN learns nonlinear relationships between extracted features and usage behavior.
- By comparing learned patterns, the model accurately identifies suspicious consumption.

H. Outcome

This mathematical model provides a structured foundation for electricity theft detection by combining statistical analysis with ANN-based learning. It ensures accurate classification, scalability, and adaptability to evolving consumption patterns in smart grid environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

V. SYSTEM DESIGN

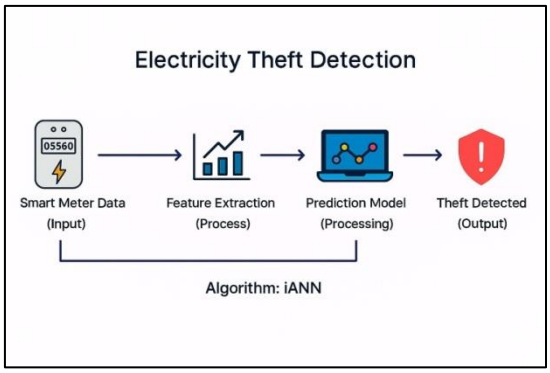


Fig.2 System Architecture

The system for detecting electricity theft in smart grids using AI begins with the collection of input data from smart meters, commonly referred to as Advanced Metering Infrastructure (AMI). These smart meters generate high-resolution, time-stamped consumption data that includes essential electrical parameters such as voltage, current, and power factor (V, I, cos φ). Additional details like the load profile (kWh data recorded every 15 minutes), tamper event flags, and power-quality indicators provide a comprehensive overview of each consumer's electricity usage. This raw data acts like the "CCTV footage" of the grid, capturing detailed usage behavior for every household or commercial unit.

The next critical stage is feature extraction, where meaningful patterns are distilled from the raw consumption data. Various types of features are computed to detect abnormalities associated with electricity theft. These include:

- **Statistical features** such as mean, variance, and skewness of the load profile.
- **Waveform anomalies**, including phase-angle changes or harmonic distortion.
- **Behavioral patterns** like unusual night-time consumption or irregular usage cycles.
- **Comparative deviations**, where a user's consumption is compared to neighborhood averages.

This process acts like a forensic investigation—identifying "cut wires" or "meter bypass" indicators that wouldn't be obvious at first glance.

At the core of the system lies the prediction model, known as iANN (intelligent Artificial Neural Network), which is a hybrid of Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), and an Attention mechanism. The CNN layers analyze spatial usage patterns in the data snapshots, the LSTM layers capture temporal sequences and detect anomalies over time, and the Attention mechanism pinpoints the most suspicious intervals in the data stream. Together, this hybrid model learns the "normal heartbeat" of a consumer's energy consumption and identifies any deviations that may indicate theft.

VI. RESULT

The proposed Electricity Theft Detection System was evaluated using real consumption data and multiple performance metrics to verify its accuracy, reliability, and practical applicability. The results include system-level outputs from the web application as well as machine learning evaluation results obtained during model training and testing. Each figure demonstrates a different aspect of system performance and is discussed in sequential order.

Fig. 2: Home Page of Electricity Theft Detection System

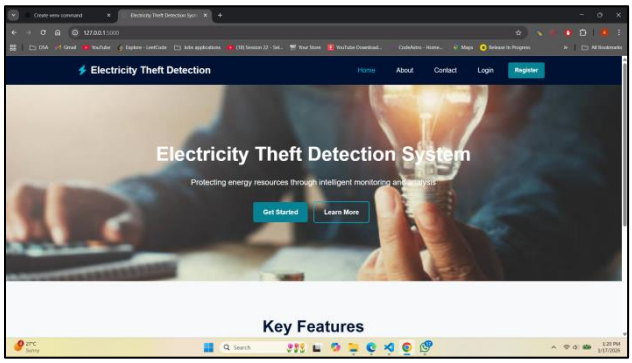


Fig 3: Home page

Fig. 2 shows the home page of the Electricity Theft Detection System developed using a Flask-based web framework. The interface provides navigation options such as Home, About, Contact, Login, and Register, ensuring secure access for users. The landing page clearly states the purpose of the system, which is to protect energy resources through intelligent monitoring and analysis. This result confirms that the system supports real-world deployment with a user-friendly and structured interface.

Fig. 3: Electricity Theft Detection Result Page

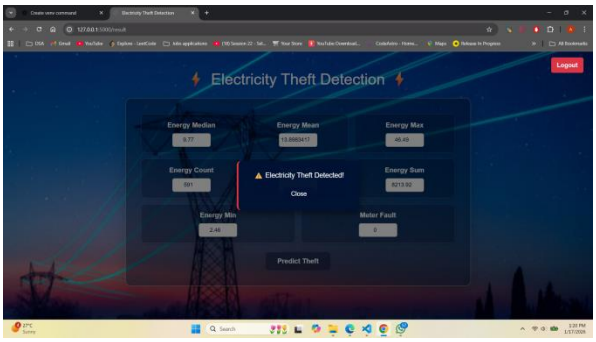


Fig 4: Result Page

Fig. 3 illustrates the prediction result page of the system after submitting energy consumption parameters. The system displays extracted statistical features including energy median, energy mean, energy maximum, energy minimum, energy sum, energy count, and meter fault status. Based on these values, the trained model classifies the consumption pattern and generates a warning message stating "Electricity Theft Detected!". This result demonstrates the effectiveness of the proposed model in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

identifying abnormal electricity usage and providing real-time alerts to utility operators.

Fig. 4: XGBoost Training vs Validation Accuracy

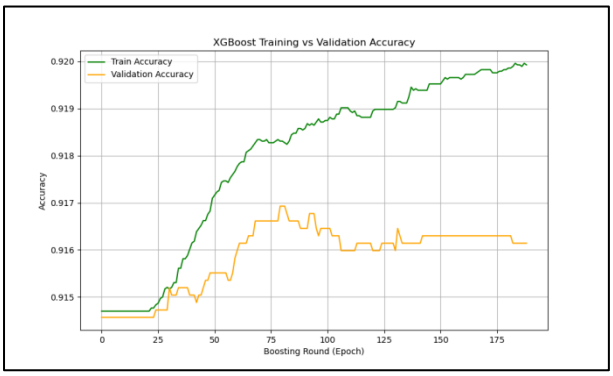


Fig 5: Training Accuracy And Validation Accuracy

Fig. 4 presents the comparison between training accuracy and validation accuracy over multiple boosting rounds during model training. The training accuracy shows a steady increase, indicating that the model successfully learns from the training data. The validation accuracy follows a stable trend close to the training curve, which indicates good generalization performance. The small gap between the two curves confirms that overfitting is minimal and the model performs consistently on unseen data.

Fig. 5: Confusion Matrix for Electricity Theft Detection

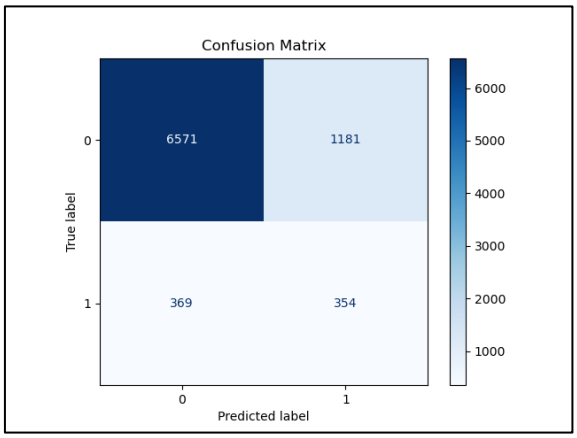


Fig 6: confusion matrix

Fig. 5 shows the confusion matrix generated from the test dataset to evaluate classification performance. The matrix indicates a high number of correctly classified normal and theft cases, demonstrating the effectiveness of the model. The presence of some false positives and false negatives reflects real-world complexity in consumption behavior; however, the overall classification balance confirms reliable detection capability. This result highlights the model's ability to distinguish between normal and fraudulent electricity usage patterns.

Fig. 6: XGBoost Training vs Validation Loss

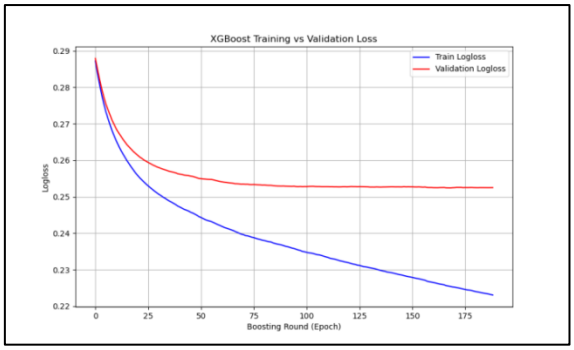


Fig 7: Training vs Validation Loss

Fig. 6 illustrates the training and validation log loss values across boosting rounds. The training loss consistently decreases, indicating effective learning by the model. The validation loss decreases initially and then stabilizes, showing that the model achieves convergence without significant overfitting. This behavior confirms that the trained model is stable, well-optimized, and suitable for deployment in practical electricity theft detection systems.

Overall Performance Analysis

The combined results from the web application output, accuracy trends, confusion matrix, and loss analysis confirm that the proposed Electricity Theft Detection System performs effectively and reliably. The system accurately detects suspicious consumption patterns, maintains stable performance on unseen data, and provides real-time alerts through a user-friendly interface. These results validate the use of machine learning techniques for reducing non-technical losses and enhancing security in smart grid environments.

VII. CONCLUSION

This project successfully presented an intelligent and automated approach for detecting electricity theft in smart grids using Artificial Intelligence techniques. By leveraging smart meter data and an Artificial Neural Network–based detection model, the system effectively identifies abnormal consumption patterns that indicate potential electricity theft. The proposed framework overcomes the limitations of traditional inspection-based and rule-based methods by providing a data-driven, scalable, and accurate solution capable of handling large volumes of consumption data generated in modern power distribution networks.

The integration of robust data preprocessing, feature extraction, and ANN-based classification ensures reliable detection performance with reduced false alarms. The inclusion of a Flask-based web application enhances system usability by enabling real-time predictions and easy interpretation of results for utility personnel. Overall, the proposed system contributes to minimizing non-technical losses, improving grid reliability, and supporting proactive decision-making for power utilities. The project demonstrates the practical applicability of AI in smart grid security and establishes a strong foundation for future

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

enhancements and wider deployment in real-world electricity distribution systems.

VIII. FUTURE SCOPE

The proposed electricity theft detection system can be further enhanced by incorporating advanced deep learning architectures such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, or hybrid models to better capture spatial and temporal consumption patterns. Integrating real-time data streaming from smart meters using IoT platforms can enable continuous monitoring and instant theft detection. Additionally, expanding the feature set to include power quality parameters, tamper event logs, and neighborhood-level comparisons can further improve detection accuracy and reduce false positives.

Future development can also focus on improving system adaptability by employing online learning or reinforcement learning techniques. Such approaches would allow the model to dynamically learn from new consumption behaviors and emerging theft strategies without requiring complete retraining. Incorporating explainable AI techniques can help utilities understand model decisions, increasing trust and facilitating regulatory compliance. Privacy-preserving methods such as federated learning can also be explored to ensure consumer data security while enabling collaborative model training across multiple utility providers.

From a deployment perspective, the system can be scaled for large-scale smart grid environments by integrating cloud-based platforms and big data processing frameworks. Mobile and dashboard-based interfaces can be developed to provide field engineers with instant alerts and actionable insights. Furthermore, the core anomaly detection framework can be adapted to other domains such as water theft detection, gas consumption monitoring, and financial fraud detection, extending the applicability and impact of the proposed system beyond electricity theft prevention.

IX. REFERENCES

[1] Depuru, L. Wang, and V. Devabhaktuni, “Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft,” Energy Policy, vol. 39, no. 2, pp. 1007–1015, 2011.

[2] N. Jokar, N. Arianpoo, and V. C. M. Leung, “Electricity theft detection in advanced metering infrastructure using customers’ consumption patterns,” IEEE Transactions on Smart Grid, vol. 6, no. 1, pp. 216–226, 2015.

[3] Z. Zheng, Y. Yang, X. Niu, H. Dai, and Y. Zhou, “Wide and deep convolutional neural networks for electricity theft detection,” CSEE Journal of Power and Energy Systems, vol. 4, no. 3, pp. 392–402, 2018.

[4] Mashima and A. A. Cárdenas, “Evaluating electricity theft detectors in smart grid networks,” in Research in Attacks, Intrusions and Defenses, Springer, pp. 210–229, 2012.

[5] M. Nizar, Z. Y. Dong, and Y. Wang, “Power utility non-technical loss analysis with extreme learning machine method,” IEEE Transactions on Power Systems, vol. 23, no. 3, pp. 946–955, 2008.

[6] H. Yang, Z. Huang, J. Lin, and Y. Chen, “Detecting electricity theft using AMI data and machine learning,” IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2831–2841, 2019.

[7] F. Javed, N. Arshad, F. Wallin, I. Khokhar, and A. Ahmed, “Forecasting electricity consumption using neural networks and smart meter data,” Applied Energy, vol. 128, pp. 331–336, 2014.

[8] Jain, A. Goel, and R. Arora, “Detection of electricity theft using machine learning techniques,” Procedia Computer Science, vol. 167, pp. 1100–1109, 2020.

[9] M. E. El-Hawary, “Artificial intelligence techniques in power systems,” IEEE Power Engineering Review, vol. 21, no. 3, pp. 52–54, 2001.

[10] G. Stracqualursi, D. Cocco, and P. Meloni, “Non-technical loss detection in smart grids using data-driven approaches,” Electric Power Systems Research, vol. 189, pp. 106727, 2020.

[11] Hasnain Iftikhar, Nitasha Khan, Muhammad Amir Raza, Ghulam Abbas, Murad Khan, Mouloud Aoudia, Ezzeddine Touti, and Ahmed Emara, “Electricity theft detection in smart grid using machine learning,” Frontiers in Energy Research, vol. 12, 2024.

[12] Ahmed T. El-Toukhy, Mahmoud M. Badr, Mohamed M. E. A. Mahmoud, Gautam Srivastava, Mostafa M. Fouda, and Maazen Alsabaan, “Electricity theft detection using deep reinforcement learning in smart power grids,” IEEE Access, vol. 11, pp. 59558–59575, 2023.

[13] Inam Ullah Khan, Nadeem Javaid, C. James Taylor, and Xiandong Ma, “Robust data-driven analysis for electricity theft attack-resilient power grid,” IEEE Transactions on Power Systems, vol. 38, no. 1, pp. 537–548, 2023.

[14] Sourav Pandey, Satyam Kandpal, and Deepika Rawat, “Real-time detection of energy theft in smart grids using machine learning,” International Journal of Research Publication and Reviews, vol. 6, no. 5, pp. 15035–15039, 2025.

[15] Sripavan B, Numair Shaikh, Spandan M N, Ananya Richu, and Elaiyaraja P, “Real-time smart grid identification: AI-enabled electricity theft detection,” Journal of Emerging Technologies and Innovative Research (JETIR), vol. 11, no. 5, 2024.

[16] K. Zidi, A. Moulahi, and H. Alaya, “Fault detection in smart grid using machine learning,” Renewable and Sustainable Energy Reviews, vol. 85, pp. 1–13, 2018.

[17] Y. Liu, Q. Chen, and X. Zhang, “Electricity theft detection in smart grid based on deep learning,” Energies, vol. 12, no. 17, pp. 3312, 2019.

[18] S. Singh and S. Yassine, “Anomaly detection for electricity theft using data mining techniques,” International Journal of Electrical Power & Energy Systems, vol. 112, pp. 158–168, 2019.

[19] Asif, Z. Wang, and S. Hussain, “Hybrid deep learning models for non-technical loss detection in smart grids,” IEEE Systems Journal, vol. 16, no. 2, pp. 2154–2163, 2022.

[20] J. Li, Y. Huang, and X. Li, “Electricity theft detection based on feature engineering and machine learning,”

[21] Energy Reports, vol. 7, pp. 456–465, 2021.