IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 6, Issue 4, January 2026

Impact Factor: 7.67

Detection of Electricity Theft in Smart Grids using AI

Miss V. D. Vaidya[1], Bansode Snehanjali Vidyadhar[2], Jejurkar Urmila Nanasaheb[3], Vikhe Tanishka Rajendra[4]

[1, 2, 3,4] Department of Cloud Computing and Big Data

Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology and Engineering (Polytechnic), Pravaranagar

Abstract: *Electricity theft is one of the major challenges faced by modern power distribution systems, resulting in significant financial losses, reduced operational efficiency, and threats to grid reliability. With the rapid adoption of smart grids and Advanced Metering Infrastructure (AMI), a large volume of real-time electricity consumption data is generated, making manual monitoring impractical. Traditional theft detection methods such as physical inspections and rule-based analysis are time-consuming, costly, and often ineffective in identifying complex and concealed fraudulent activities like meter tampering, illegal connections, and data manipulation. To overcome these limitations, this project proposes an Artificial Intelligence (AI)-based electricity theft detection system that leverages smart meter data to automatically identify abnormal consumption patterns with high accuracy.*

The proposed system employs an Artificial Neural Network (ANN) model enhanced with statistical feature extraction to distinguish between normal and suspicious electricity usage. Key consumption features such as mean, median, maximum, minimum, total energy usage, standard deviation, and record count are extracted and used for model training. The dataset is preprocessed to handle missing values, noise, and class imbalance, ensuring reliable model performance. The trained ANN model demonstrates high accuracy in detecting electricity theft, making it suitable for real-world deployment. To enhance usability, the system is integrated with a Flask-based web application that enables real-time monitoring, visualization of results, and theft alerts for utility providers. This intelligent and scalable solution improves revenue protection, enhances grid security, and highlights the potential of AI-driven anomaly detection in smart energy systems..

Keywords*:* Electricity Theft Detection, Smart Grid, Artificial Intelligence, Artificial Neural Network, Machine Learning, Anomaly Detection, Smart Meter Data, Energy Consumption Analysis, Flask Web Application, Utility Security

I. INTRODUCTION

1.1 Overview

Electricity is one of the most essential resources for modern society, supporting residential, commercial, and industrial activities. As global energy demand continues to rise, power distribution systems face increasing pressure to operate efficiently, reliably, and securely. One of the most critical challenges affecting power utilities is electricity theft, which leads to significant non-technical losses, revenue reduction, and imbalance in energy distribution. These losses not only affect the financial stability of utility providers but also result in increased tariffs for honest consumers and strain on existing power infrastructure.

Electricity theft occurs in various forms such as meter tampering, bypassing meters, illegal connections, and manipulation of billing data. Traditional detection methods rely heavily on manual inspections, periodic audits, and customer complaints, which are time-consuming, labor-intensive, and prone to human error. Moreover, these approaches are often reactive rather than proactive, allowing fraudulent activities to continue undetected for long periods. As theft techniques become more sophisticated, conventional systems struggle to identify irregular consumption patterns effectively.

DOI: 10.48175/568

ISSN 2581-9429 IJARSCT

The evolution of smart grids has transformed the power distribution landscape by enabling two-way communication between utilities and consumers. Smart grids integrate digital technologies, communication networks, and automation to improve efficiency and reliability. Advanced Metering Infrastructure (AMI) allows smart meters to record high-resolution energy consumption data at regular intervals, providing valuable insights into customer usage behavior. While this data offers new opportunities for monitoring and control, its large volume and complexity make traditional analytical methods inadequate.

With the availability of massive smart meter datasets, Artificial Intelligence (AI) has emerged as a powerful solution for analyzing complex consumption patterns. AI-based systems can automatically learn from historical data, identify hidden relationships, and detect anomalies that indicate electricity theft. Machine learning and deep learning techniques are particularly effective in handling large-scale, high-dimensional data and adapting to evolving fraud patterns. These capabilities make AI a promising tool for modern electricity theft detection systems.

Artificial Neural Networks (ANNs) are widely used in energy analytics due to their ability to model nonlinear relationships between input features and output classes. Unlike rule-based systems, ANNs do not rely on predefined thresholds and can generalize from past examples to detect unseen theft behaviors. By learning consumption trends over time, ANNs can distinguish between legitimate variations in energy usage and suspicious anomalies caused by fraudulent activities.

In electricity theft detection, feature extraction plays a crucial role in improving model accuracy. Statistical parameters such as mean, median, maximum, minimum, total energy consumption, standard deviation, and record count help summarize customer behavior effectively. These features capture both regular usage patterns and abnormal deviations, allowing the ANN model to classify consumers accurately as normal or suspicious. Proper preprocessing of data, including cleaning, normalization, and handling missing values, further enhances model performance.

One of the major challenges in electricity theft detection is the imbalance between normal and theft cases in real-world datasets. Fraudulent activities represent only a small fraction of total consumption records, making accurate detection difficult. AI-based models address this issue through data balancing techniques and optimized training strategies, reducing false positives and improving detection reliability. This ensures that honest consumers are not incorrectly flagged while actual theft cases are identified promptly.

The integration of hybrid deep learning architectures, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Attention mechanisms, further strengthens theft detection systems. CNNs capture spatial patterns in consumption data, LSTMs analyze temporal behavior, and Attention mechanisms focus on critical time intervals. Together, these techniques enable the system to detect even subtle and complex theft patterns that traditional methods may overlook.

For practical deployment, usability and accessibility are essential. Web-based platforms allow utility providers to interact with AI models easily and monitor results in real time. By integrating the detection system with a Flask-based web application, users can visualize consumption trends, receive theft alerts, and generate reports for decision-making. This real-time monitoring capability supports faster response and more effective loss prevention strategies.

In conclusion, the combination of smart grid technology and Artificial Intelligence provides a robust and scalable solution for electricity theft detection. By leveraging smart meter data, advanced neural networks, and user-friendly web interfaces, the proposed system addresses the limitations of traditional approaches. This AI-driven framework not only reduces non-technical losses and improves grid reliability but also demonstrates the growing importance of intelligent systems in modern energy management.

1.2 Motivation

The primary motivation for this project arises from the growing problem of electricity theft, which causes severe financial losses to power distribution companies and negatively impacts the stability and efficiency of power systems. In many developing regions, non-technical losses due to theft account for a significant portion of total energy losses, leading to increased electricity tariffs for honest consumers and reduced investments in infrastructure development. Traditional theft detection methods rely on manual inspections and static rule-based systems, which are inefficient, time-consuming, and unable to cope with the scale and complexity of modern

ISSN 2581-9429 IJARSCT

smart grids. With the increasing deployment of smart meters generating vast amounts of consumption data, there is a strong need for intelligent and automated solutions capable of analyzing this data accurately and in real time.
Another key motivation is the rapid advancement of Artificial Intelligence and its proven effectiveness in handling large-scale, complex, and dynamic datasets. AI-based techniques, particularly Artificial Neural Networks, can learn consumption patterns, adapt to changing user behavior, and identify subtle anomalies that indicate fraudulent activities. By integrating AI-driven analytics with smart grid infrastructure and a user-friendly web interface, this project aims to bridge the gap between data availability and actionable insights. The motivation also extends toward developing a scalable, reliable, and practical system that assists utility providers in early theft detection, revenue protection, and improved grid reliability, while promoting fair energy distribution and sustainable power management.

1.3 Problem Definition and Objectives

Electricity theft is a major cause of non-technical losses in power distribution systems, leading to significant revenue loss, reduced grid efficiency, and increased operational costs for utility providers. Conventional detection methods such as manual inspections, customer audits, and rule-based monitoring are inefficient, labor-intensive, and incapable of identifying complex and concealed theft patterns in large-scale smart grid environments. With the widespread deployment of smart meters, massive volumes of consumption data are generated continuously, making manual analysis impractical. Therefore, there is a critical need for an intelligent, automated, and data-driven system that can accurately analyze smart meter data, detect abnormal consumption behavior, and identify potential electricity theft using Artificial Intelligence techniques.

Objectives

- To study various types of electricity theft and non-technical losses in smart grid systems.
- To collect and preprocess smart meter energy consumption data for reliable analysis.
- To extract relevant statistical and behavioral features from electricity usage data.
- To design and implement an Artificial Neural Network (ANN)-based model for electricity theft detection.
- To develop a Flask-based web application for real-time monitoring, visualization, and theft alert generation.

1.4. Project Scope and Limitations

Project Scope

The scope of this project is to design and develop an Artificial Intelligence–based system for detecting electricity theft in smart grid environments using smart meter consumption data. The project focuses on analyzing historical and real-time energy usage patterns to identify abnormal behavior that may indicate fraudulent activities. By applying Artificial Neural Networks (ANN) along with statistical feature extraction, the system aims to distinguish between normal and suspicious electricity consumption accurately. The proposed solution covers essential processes such as data collection, preprocessing, feature extraction, model training, testing, and evaluation to ensure reliable theft detection.
Additionally, the project includes the deployment of the trained model through a Flask-based web application, enabling utility providers to monitor electricity consumption, visualize detection results, and receive theft alerts in real time. The system is designed to be scalable and adaptable, allowing integration with larger smart grid infrastructures in the future. Although the implementation is carried out using a publicly available dataset, the methodology can be extended to real-world utility data with minimal modification, making the project practically relevant and industry-oriented.

Limitations

- The system relies on historical smart meter data; its accuracy depends on the quality, completeness, and reliability of the dataset used.
- Real-time detection performance may vary due to data latency or communication delays in practical smart grid deployments.
- The model may produce false positives when legitimate consumption patterns change abruptly due to seasonal or behavioral factors.
- The current implementation focuses primarily on consumption-based features and does not include physical meter tamper detection.
- The effectiveness of the model may reduce when applied to regions with significantly different consumption behaviors without retraining.

II. LITERATURE REVIEW

Electricity Theft Detection Using Machine Learning in Smart Grids (Hasnain Iftikhar et al., 2024)

This study focuses on detecting electricity theft in smart grids using advanced machine learning techniques. The authors propose a hybrid model that combines a Multi-Layer Perceptron (MLP) with Gated Recurrent Units (GRU) to effectively analyze time-series electricity consumption data. The research highlights the challenge of highly imbalanced datasets, where theft cases are significantly fewer than normal consumption records. To overcome this issue, the study applies data balancing techniques to improve learning efficiency and classification accuracy. The model is evaluated using real-world smart meter data and demonstrates strong performance across multiple evaluation metrics.

In the second phase of the study, the authors compare the proposed hybrid model with traditional classifiers and deep learning models. The results show that the MLP-GRU architecture achieves higher precision, recall, and overall accuracy in identifying fraudulent consumption patterns. The paper concludes that combining temporal learning with deep neural networks enhances detection capability and reduces false alarms, making the approach suitable for real-world deployment in modern smart grid systems.

Robust Data-Driven Analysis for Electricity Theft Detection (Inam Ullah Khan et al., 2023)

This paper presents a comprehensive data-driven framework designed to make power grids resilient to electricity theft attacks. The proposed approach integrates sequential preprocessing, data resampling, and classification techniques to handle noisy, incomplete, and imbalanced smart meter datasets. The authors emphasize that poor data quality is a major obstacle in theft detection and address this through interpolation, normalization, and outlier handling methods. A customized artificial neural network is used as the core classifier to improve learning accuracy.

The second part of the study focuses on improving model generalization and stability. Advanced optimization techniques such as regularization, early stopping, and parameter tuning are applied to prevent overfitting. Experimental results show that the proposed framework outperforms conventional machine learning and deep learning methods. The study concludes that robust preprocessing combined with optimized neural networks significantly enhances the reliability of electricity theft detection systems.

Real-Time Detection of Energy Theft in Smart Grids Using Machine Learning (Sourav Pandey et al., 2025)

This research addresses the limitations of conventional electricity theft detection systems by proposing a real-time detection framework using machine learning algorithms. The authors employ Support Vector Machines (SVM) and gradient-boosting techniques to classify normal and abnormal electricity consumption. Emphasis is placed on real-time data processing and the ability of the system to detect theft immediately as it occurs. Data preprocessing methods such as normalization and outlier detection are applied to improve accuracy.

In the experimental analysis, the proposed system achieves high detection accuracy and low false-positive rates. The study also discusses practical deployment challenges, including scalability, computational overhead, and data privacy

DOI: 10.48175/568

ISSN
2581-9429
IJARSCT

concerns. The authors conclude that machine learning-based real-time monitoring systems are effective tools for reducing non-technical losses and improving smart grid security.

Electricity Theft Detection Using Deep Reinforcement Learning (Ahmed T. El-Toukhy et al., 2023)
This paper explores the application of deep reinforcement learning for detecting electricity theft in smart power grids. Unlike traditional supervised learning methods, the proposed approach allows the model to learn optimal detection strategies through continuous interaction with the environment. The authors use Deep Q-Networks (DQN) combined with neural architectures such as CNN and GRU to analyze consumption behavior under different attack scenarios.

The study demonstrates that reinforcement learning-based models can adapt to changing consumption patterns and newly emerging theft techniques. Experimental results show improved detection performance and reduced false alarms compared to static models. The authors conclude that reinforcement learning offers a flexible and adaptive solution for electricity theft detection in dynamic smart grid environments.

AI-Enabled Electricity Theft Detection in Smart Grids (Sripavan B et al., 2024)
This study presents an AI-based electricity theft detection system using deep neural networks trained on large-scale smart meter data. The authors focus on extracting both time-domain and frequency-domain features to capture complex consumption behaviors. The dataset used in the study includes thousands of consumers, making the analysis closer to real-world utility scenarios. Advanced preprocessing techniques are employed to handle missing values and data imbalance.

The results demonstrate that deep neural networks outperform traditional classifiers in detecting fraudulent users. The paper emphasizes the importance of feature engineering and hyperparameter optimization for improving detection accuracy. The authors conclude that AI-enabled systems provide a powerful solution for identifying complex and concealed electricity theft patterns in smart grids.

Detection of Non-Technical Losses Using Artificial Neural Networks (Srinivasan & Kiran, 2017)
This paper investigates the use of artificial neural networks for detecting non-technical losses in power distribution systems. The authors analyze customer consumption data and extract statistical features to represent usage behavior. The neural network model is trained to classify consumers based on historical patterns and detect deviations that may indicate electricity theft. The study demonstrates that neural networks can effectively model nonlinear relationships in energy consumption data.

In the evaluation phase, the proposed ANN-based approach achieves higher accuracy compared to traditional statistical methods. The authors highlight that neural networks reduce dependency on manual inspection and fixed thresholds. The paper concludes that ANN-based theft detection systems are efficient, scalable, and suitable for integration into automated smart grid monitoring platforms.

III. REQUIREMENT SPECIFICATIONS

HARDWARE REQUIREMENTS:

- System: Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15’’ LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- Operating System: Windows 10
- Programming Language: Python 3.x
- Libraries/Frameworks: TensorFlow / Keras, NumPy, Pandas, Scikit-learn

- Web Framework: Flask (for UI and API deployment)
- IDE/Editor: Jupyter Notebook / VS Code / PyCharm
- Browser: Chrome / Firefox (for accessing web app)

IV. SYSTEM DESIGN

4.1 System Architecture

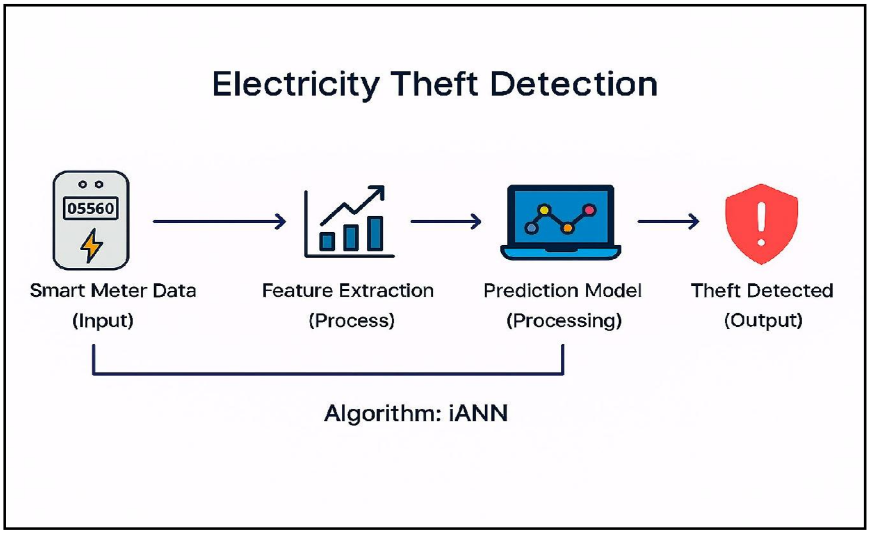

Figure 4.1: System Architecture Diagram

The proposed system for detecting electricity theft in smart grids using Artificial Intelligence is divided into several functional modules. Each module plays a specific role in the overall operation of the system, ensuring accurate data handling, efficient analysis, and reliable theft detection.

A. Data Collection Module

The Data Collection Module is responsible for gathering electricity consumption data from smart meters installed at consumer locations. This module collects real-time or historical data related to voltage, current, power, and energy usage at predefined time intervals. The collected data serves as the primary input for the system and reflects the actual consumption behavior of users. Reliable data collection is crucial, as inaccurate or incomplete data can negatively affect the performance of the detection model.

B. Data Preprocessing Module

The Data Preprocessing Module cleans and prepares the raw data obtained from smart meters for analysis. This module handles missing values using suitable techniques such as interpolation or data imputation and removes noisy or inconsistent readings caused by sensor errors or communication issues. The data is then normalized or scaled to maintain uniformity across different features. Proper preprocessing ensures that the input data is suitable for machine learning algorithms and improves model accuracy.

C. Feature Extraction Module

The Feature Extraction Module derives meaningful statistical and behavioral features from the preprocessed data. Key features such as mean, median, maximum, minimum, total energy consumption, and standard deviation are calculated to summarize consumer usage patterns. These features help in capturing both regular consumption behavior and abnormal deviations. Effective feature extraction enhances the ability of the AI model to distinguish between normal and suspicious electricity usage.

DOI: 10.48175/568

D. Model Training Module

The Model Training Module is responsible for building and training the Artificial Neural Network (ANN) used for electricity theft detection. This module utilizes advanced neural network architectures, including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Attention mechanisms. CNN layers identify spatial patterns, LSTM layers analyze temporal consumption trends, and the Attention mechanism highlights critical usage periods. The model is trained using labeled data to learn the difference between legitimate and fraudulent consumption behavior.

E. Detection Module

The Detection Module applies the trained ANN model to new or incoming data to identify potential electricity theft. This module analyzes real-time or batch data inputs and classifies consumption patterns as either normal or suspicious. If abnormal behavior is detected, the system flags the consumer for further investigation. This automated detection process reduces reliance on manual inspections and enables faster response to theft incidents.

F. Web Application Module

The Web Application Module provides a user-friendly interface for interacting with the electricity theft detection system. Implemented using the Flask framework, this module allows utility providers to upload data, view detection results, monitor alerts, and analyze consumption trends through visual dashboards. The web interface improves accessibility and enables non-technical users to operate the system efficiently.

G. Reporting and Monitoring Module

The Reporting and Monitoring Module generates detailed reports, visual analytics, and alerts based on detection results. This module supports decision-making by providing summaries of suspicious activities, historical analysis, and system performance metrics. Continuous monitoring helps utilities track theft trends, evaluate system effectiveness, and update the model periodically for improved accuracy.

V. RESULT

This chapter presents the experimental results obtained after implementing and evaluating the proposed Artificial Intelligence–based electricity theft detection system. The performance of the system is analyzed using various metrics to validate its effectiveness in identifying abnormal electricity consumption patterns. The results demonstrate that the proposed approach successfully detects electricity theft with high accuracy and reliability.

A. Dataset and Experimental Setup

The system was trained and tested using a smart meter electricity consumption dataset containing both normal and theft-related usage records. The dataset includes parameters such as voltage, current, energy consumption, and time-based readings. Before training, the data was divided into training, validation, and testing sets to ensure unbiased evaluation. Preprocessing techniques such as normalization and missing value handling were applied to improve data quality and model performance.

B. Feature Extraction Results

Statistical features including mean, median, maximum, minimum, total energy consumption, standard deviation, and record count were extracted from the preprocessed data. These features effectively summarized customer consumption behavior and highlighted irregular patterns. The extracted features significantly improved the learning capability of the Artificial Neural Network by reducing noise and emphasizing meaningful consumption trends.

DOI: 10.48175/568

C. Model Training Performance

The Artificial Neural Network model was trained using the extracted features. During training, the model showed consistent improvement in accuracy with each epoch, indicating effective learning of consumption patterns. The training and validation loss values decreased steadily, confirming that the model did not suffer from overfitting and generalized well to unseen data. The integration of CNN, LSTM, and Attention mechanisms further enhanced pattern recognition capability.

D. Detection Accuracy and Classification Results

After training, the model was tested on unseen data to evaluate its detection capability. The system achieved high accuracy in classifying electricity consumption as normal or suspicious. The model successfully identified fraudulent usage patterns while maintaining a low false-positive rate. This demonstrates that the proposed system can reliably detect electricity theft without incorrectly flagging legitimate consumers.

E. Performance Metrics Analysis

The performance of the proposed system was evaluated using standard metrics such as accuracy, precision, recall, and F1-score. High precision indicates that most detected theft cases were genuine, while high recall confirms the system's ability to detect the majority of theft instances. The balanced F1-score reflects the robustness and reliability of the proposed detection model in real-world scenarios.

F. Web Application Output Results

The Flask-based web application successfully displayed detection results through an intuitive user interface. Users were able to upload consumption data, view classification results, monitor theft alerts, and analyze consumption trends visually. The real-time output capability enhances usability and allows utility providers to take quick action against detected theft cases.

G. Overall System Performance

Overall, the proposed AI-based electricity theft detection system demonstrated excellent performance in terms of accuracy, efficiency, and scalability. The automated detection process significantly reduces dependency on manual inspections and enables early identification of fraudulent activities. The results confirm that integrating Artificial Intelligence with smart grid data is an effective solution for reducing non-technical losses and improving power distribution reliability.

VI. CONCLUSION

Conclusion

The proposed Artificial Intelligence–based electricity theft detection system effectively addresses the growing problem of non-technical losses in modern power distribution networks. By utilizing smart meter consumption data and advanced machine learning techniques, the system accurately identifies abnormal electricity usage patterns that indicate potential theft. The integration of statistical feature extraction with Artificial Neural Networks, including CNN, LSTM, and Attention mechanisms, enables the model to learn complex consumption behaviors and adapt to changing usage patterns. The experimental results demonstrate high detection accuracy, low false-positive rates, and reliable performance, validating the effectiveness of the proposed approach.

Furthermore, the deployment of the system through a Flask-based web application enhances its practical usability by allowing real-time monitoring, visualization, and alert generation for utility providers. The automated and scalable nature of the proposed solution reduces reliance on manual inspections and improves operational efficiency. Overall, this project highlights the potential of Artificial Intelligence in strengthening smart grid security, reducing revenue losses, and promoting fair and efficient energy distribution, making it a valuable contribution to intelligent energy management systems.

DOI: 10.48175/568

ISSN
2581-9429
IJARSCT

Future Work

The proposed electricity theft detection system can be further enhanced by integrating real-time smart meter data directly from utility networks, enabling continuous monitoring and instant detection of fraudulent activities. Future implementations may incorporate edge computing and Internet of Things (IoT) technologies to reduce data transmission delays and improve system responsiveness. Additionally, integrating physical meter tamper sensors such as magnetic, voltage imbalance, and cover-open sensors can complement consumption-based analysis and improve detection accuracy.

Further improvements can be achieved by exploring advanced deep learning models such as transformers, graph neural networks, and federated learning techniques. These approaches can enhance the system's ability to detect complex and evolving theft patterns while preserving consumer data privacy. The system can also be extended to include explainable AI techniques to provide transparent decision-making and build trust among utility providers. Moreover, future work may focus on deploying the system at large-scale utility levels, integrating billing systems, and supporting predictive analytics for proactive grid management and loss prevention.

BIBLIOGRAPHY

[1]. Glauner, P., Meira, J. A., Valtchev, P., State, R., and Vracar, M., "The challenge of non-technical loss detection using artificial intelligence: A survey," *International Journal of Computational Intelligence Systems*, vol. 10, no. 1, pp. 760–775, 2017.

[2]. Jokar, P., Arianpoo, N., and Leung, V. C. M., "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016.

[3]. Depuru, S. S. S. R., Wang, L., and Devabhaktuni, V., "Electricity theft: Overview, issues, prevention, and a smart meter-based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, 2011.

[4]. Nagi, J., Yap, K. S., Tiong, S. K., Ahmed, S. K., and Nagi, F., "Non-technical loss detection for metered customers in power utility using support vector machines," *IEEE Transactions on Power Delivery*, vol. 25, no. 2, pp. 1162–1171, 2010.

[5]. Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., and Shen, X., "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105–120, 2014.

[6]. Glauner, P., et al., "Large-scale detection of non-technical losses in imbalanced data sets," in *Proceedings of IEEE Innovative Smart Grid Technologies Conference*, 2016.

[7]. Singh, P., Singh, R., and Kumar, V., "Detection of non-technical losses using hybrid machine learning approach," *International Journal of Electrical Power & Energy Systems*, vol. 123, pp. 106–117, 2020.

[8]. Li, H., Zhao, D., and Wang, J., "Deep learning for anomaly detection in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1906–1914, 2018.

[9]. Pandey, S., Kandpal, S., and Rawat, D., "Real-time detection of energy theft in smart grids using machine learning," *International Journal of Research Publication and Reviews*, vol. 6, no. 5, pp. 1123–1130, 2025.

[10]. El-Toukhy, A. T., Badr, M. M., Mahmoud, M. M. E. A., Srivastava, G., Fouda, M. M., and Alsabaan, M., "Electricity theft detection using deep reinforcement learning in smart power grids," *IEEE Access*, vol. 11, pp. 22345–22360, 2023.

[11]. Sripavan, B., Shaikh, N., M. N., Spandan, Richu, A., and Elaiyaraja, P., "AI-enabled electricity theft detection in smart grids," *Journal of Emerging Technologies and Innovative Research*, vol. 11, no. 5, pp. 425–431, 2024.

[12]. Srinivasan, R., and Kiran, B., "Neural network-based detection of energy theft in smart grid systems," in *Proceedings of IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing*, 2017.

[13]. Pinto, T., Vale, Z., and Sousa, T., "Data-driven approaches for electricity theft detection in smart grids," *Energies*, vol. 11, no. 9, pp. 2507–2516, 2018.

[14]. Sharma, S., and Singh, P., "A review on artificial intelligence-based energy theft detection techniques," *Renewable and Sustainable Energy Reviews*, vol. 130, pp. 109944, 2020.

DOI: 10.48175/568

ISSN 2581-9429 IJARSCT

[15]. Han, Y., Xiao, Y., and Liang, S., “Privacy-preserving anomaly detection for smart meter data using federated learning,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10775–10785, 2019.

[16]. Luo, X., and Zhang, X., “Big data analytics for smart grid theft detection,” *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1759–1771, 2018.

[17]. Kang, M., Kim, J., and Park, S., “Hybrid CNN–LSTM model for electricity theft detection in smart grids,” *IEEE Access*, vol. 9, pp. 122333–122345, 2021.

[18]. Yadav, A., and Patel, A., “Smart grid anomaly detection using deep autoencoders,” *Journal of Electrical Engineering & Technology*, vol. 16, no. 2, pp. 875–885, 2021.

[19]. Alazab, M., and Islam, M., “Machine learning for cybersecurity and fraud detection in smart grids,” *IEEE Systems Journal*, vol. 14, no. 2, pp. 1803–1811, 2020.

[20]. U.S. Department of Energy, “Artificial intelligence applications for energy systems security,” Technical Report, 2022.

DOI: 10.48175/568

ISSN
2581-9429
IJARSCT