International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Smart Electricity Theft Detection Using AI and IoT with Auto Power Cut and Web Monitoring

Vasanthakumar. C[1], Mohan Raj. M[2], Janaki. K[3], Karthika. S[4], Dinesh Vishnu. M[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Angel College of Engineering and Technology, Tirupur, India
[2,3,4,5]Final Year UG Scholar, Department of Electronics and Communication Engineering, Angel College of Engineering and Technology, Tirupur, India

ABSTRACT
Electricity theft is a major issue affecting power distribution systems, leading to significant financial losses and reduced efficiency. This paper presents an AI and IoT-based real-time electricity theft detection system that monitors electrical parameters such as current and voltage using sensors. The collected data is transmitted through an ESP32 microcontroller to a server for analysis. A machine learning model is used to identify abnormal consumption patterns and detect potential theft. The system also incorporates Explainable AI techniques to provide transparency in decision-making. Upon detection of theft, alerts are generated and an automatic power cut-off mechanism is triggered using a relay. A web-based dashboard is developed for real-time monitoring and visualization. The proposed system is cost-effective, accurate, and scalable for practical deployment.

Keywords: AI, IoT, Electricity Theft Detection, Machine Learning, Smart Grid, ESP32, Real-Time Monitoring.

1. INTRODUCTION
Electricity theft is one of the major challenges faced by power utilities worldwide. Traditional methods of detecting electricity theft are inefficient and often fail to identify sophisticated theft techniques. With the advancement of Internet of Things (IoT) and Artificial Intelligence (AI), it is possible to develop intelligent systems for real-time monitoring and detection.
This project proposes an AI and IoT-based system that continuously monitors electricity usage and identifies abnormal consumption patterns. The integration of machine learning enhances detection accuracy and reduces false alarms.

2. LITERATURE SURVEY
Electricity theft detection has gained significant attention due to its economic impact and challenges in power distribution systems. Various techniques have been proposed using IoT, smart meters, and machine learning approaches.

A. Smart Meter-Based Detection
Early research focused on using smart meter data to detect electricity theft. Sahoo et al. proposed a predic-

tive model using consumption data from smart meters and transformers to identify theft patterns.
Their approach demonstrated that frequent data collection enables advanced analysis and improves detection efficiency.
However, these systems mainly rely on centralized data and lack real-time response capabilities.

B. IoT-Based Electricity Theft Detection

Recent studies introduced IoT-based systems for real-time monitoring. An IoT-based smart energy meter system using Arduino and sensors was developed to monitor voltage, current, and power consumption, with data transmitted to a cloud platform for analysis. Similarly, other research highlights that IoT systems enable real-time monitoring and remote access, improving detection speed and efficiency. Despite these advantages, IoT systems alone lack intelligent decision-making and may produce false alarms.

C. Machine Learning-Based Detection

Machine learning techniques such as Decision Trees, SVM, and Neural Networks have been widely used for theft detection. Studies show that ML models can analyse consumption patterns and detect anomalies with high accuracy. Advanced models like deep learning (CNN, RNN, LSTM) further improve performance by capturing complex temporal patterns in electricity usage. However, these models require large datasets and may face issues like data imbalance and high computational cost.

D. Hybrid AI + IoT Systems

Recent research combines IoT and Machine Learning for better performance. Hybrid systems collect real-time data using IoT sensors and apply ML algorithms for anomaly detection, resulting in improved accuracy and reduced false positives. Such systems also support cloud-based analytics and scalable deployment, making them suitable for smart grid environments.

E. Research Gaps

From the literature, the following gaps are identified:

- Lack of real-time intelligent detection in traditional systems
- High false positive rates in rule-based approaches
- Limited use of Explainable AI for decision transparency
- Dependence on large datasets in ML models
- Insufficient integration of automatic control (power cut-off)

F. Summary

Existing works demonstrate that IoT enables real-time monitoring, machine learning improves detection accuracy, and hybrid approaches provide better performance. However, there is still a need for a cost-effective, real-time, explainable, and automated system — which is addressed in the proposed project.

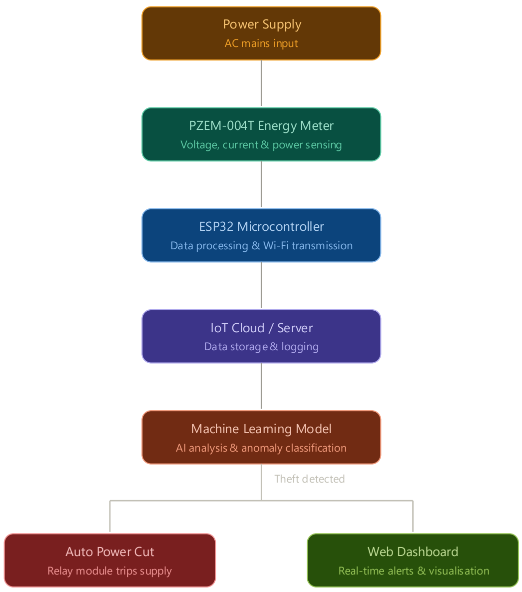
3. EXISTING SYSTEM

The existing electricity theft detection systems mainly depend on traditional approaches such as manual inspection, electromechanical meters, and basic digital energy meters. In many cases, utility personnel are required to physically monitor and inspect the meters, which is time-consuming, labour-intensive, and not suitable for large-scale deployment. With the advancement of technology, some systems have adopted smart meters and IoT-based monitoring, where electrical parameters like current and voltage are measured and transmitted to a central server. However, these systems typically rely on fixed threshold values to detect abnormal consumption, which makes them less effective in handling dynamic and varying usage patterns. As a result, they often generate false positives or fail to detect sophisticated theft techniques such as partial bypassing or meter tampering. Additionally, most existing systems lack real-time intelligent decision-making, explainability, and automated response mechanisms like power cut-off. Therefore, they are limited in terms of accuracy, reliability, and efficiency, creating a strong need for an advanced AI and IoT-based system.

4. PROPOSED SYSTEM

The proposed system presents an AI and IoT-based real-time electricity theft detection system that overcomes the limitations of traditional methods by integrating smart sensing, intelligent analysis, and automated control. In this system, electrical parameters such as current and voltage are continuously monitored using sensors like ACS712 and transmitted through an ESP32 microcontroller to a server or cloud platform. The collected data is analysed using a machine learning model, which learns normal consumption patterns and identifies abnormal behaviour that may indicate electricity theft. Unlike conventional threshold-based systems, the proposed approach provides higher accuracy and reduces false detections. Additionally, Explainable AI techniques are incorporated to understand and justify the model's decisions. The system also includes a web-based dashboard for real-time monitoring and visualization of data. When theft is detected, an alert is generated, and an automatic power cut-off mechanism is activated using a relay module. Overall, the proposed system is intelligent, cost-effective, scalable, and capable of providing reliable real-time electricity theft detection and control.

5. BLOCK DIAGRAM



[Fig. 1: Block Diagram of the Proposed System]

6. METHODOLOGY

1. **Data Collection**: Sensors such as ACS712 measure current and the PZEM-004T module measures voltage, current, power, and energy parameters, transmitting data via the ESP32 microcontroller.
2. **Data Transmission:** Data is transmitted to a cloud server or local server using Wi-Fi/GSM connectivity provided by the ESP32.
3. **Machine Learning Model:** A supervised learning model (Decision Tree or Support Vector Machine) is trained to classify electricity usage patterns as normal or theft based on collected parameters.

4. **Explainable AI:** The SHAP (Shapley Additive explanations) technique is used to interpret and justify the machine learning model's decisions, providing transparency.
5. **Action Mechanism:** Upon theft detection: an alert is generated on the web dashboard, and the relay module automatically cuts off the power supply to the affected meter.

7. CONCLUSION

This project presents an AI and IoT-based real-time electricity theft detection system that effectively addresses the limitations of traditional methods. By integrating sensors, ESP32 microcontroller, and machine learning algorithms, the system continuously monitors electrical parameters and accurately identifies abnormal consumption patterns. Unlike conventional threshold-based systems, the proposed approach provides improved accuracy, reduced false alarms, and intelligent decision-making.

The implementation of a web-based dashboard enables real-time monitoring and visualization, while the automatic power cut-off mechanism ensures immediate action upon theft detection. The inclusion of Explainable AI further enhances the transparency and reliability of the system. Overall, the proposed system is cost-effective, scalable, and efficient, making it suitable for practical deployment in modern power distribution networks.

8. FUTURE SCOPE

The proposed AI and IoT-based electricity theft detection system can be further enhanced in several ways to improve its performance, scalability, and practical implementation. In the future, advanced deep learning models such as LSTM and neural networks can be integrated to improve the accuracy of detecting complex and hidden theft patterns. The system can also be expanded into a smart grid environment, where multiple nodes are interconnected for centralized monitoring and control.

Additionally, the development of a mobile application can provide real-time alerts and remote access for users and electricity boards. Integration with renewable energy sources such as solar systems can enable better energy management and monitoring. The use of edge computing can reduce latency by processing data locally instead of relying entirely on cloud servers.

Furthermore, implementing blockchain technology can enhance data security and prevent tampering. The system can also be scaled for large-scale deployment in urban and rural areas, improving overall power distribution efficiency. Future improvements may include predictive analytics to forecast energy consumption and detect anomalies before theft occurs. Overall, the system has strong potential to evolve into a fully automated, intelligent, and secure energy management solution.

REFERENCES

1. Jamdade, K., Wetal, S., Yadav, K., Sherkhane, B., and Taware, S.,“AI-Based Electricity Theft Detection System,” *International Journal of Research Publication and Reviews (IJRPR)*,vol. 6, no. 11, pp. 6409–6413, 2025.
2. K. Y. Huang, C. H. Hsu, and Y. S. Chen, "Electricity theft detection using machine learning and deep learning techniques," International Journal of Electrical Power & Energy Systems, vol. 121, 2020.
3. H. Iftikhar, N. Khan, M. A. Raza, G. Abbas, and M. Aoudia, "Electricity theft detection in smart grid using machine learning," Frontiers in Energy Research, vol. 12, 2024.
4. Y. Zhang, Q. Ai, H. Wang, et al., "Energy theft detection using anomaly detection techniques," International Journal of Electrical Power & Energy Systems, 2024.

5. "Machine-learning techniques for enhancing electricity theft detection," Energy Reports, 2024.
6. N. M. Elshennawy, D. M. Ibrahim, and A. M. Gab Allah, "An efficient electricity theft detection based on deep learning," Scientific Reports, vol. 15, 2025.
7. X. Chen, C. Huang, Y. Zhang, and H. Wang, "Hybrid deep learning model for electricity theft detection in smart grids," arXiv preprint, 2025.
8. C. Collier and K. Guha, "Lightweight LSTM model for energy theft detection," arXiv preprint, 2025.
9. D. Labate, D. Thakur, and G. Fortino, "Federated learning approach for secure electricity theft detection," arXiv preprint, 2026.
10. A. U. Oguntola, O. A. AbdulQoyum, and A. M. Madehin, "Hybrid GNN and LSTM framework for electricity theft detection," arXiv preprint, 2026.