Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Review On Energy Theft Detection Using IOT

Sakshi Adole[1], Nishant Khule[2], Harshal Mali[3], Tejas Nandan[4], Mr. Chandrakant Aher[5]

[1, 2, 3, 4] Student, Information Technology Department, Rajarshi Shahu Maharaj Polytechnic, Nashik
[5] Lecturer, Information Technology Department, Rajarshi Shahu Maharaj Polytechnic, Nashik

Abstract

Energy theft is one of the major causes of non-technical losses in power distribution systems, leading to significant financial damage and reduced grid reliability. Conventional detection methods are largely manual, time-consuming, and ineffective against modern techniques such as meter tampering, bypass connections, and data manipulation. This project proposes an IoT-based energy theft detection system integrated with intelligent analytics to enable real-time monitoring and automated identification of fraudulent activities. Smart meters and IoT sensors continuously collect electrical parameters such as voltage, current, power factor, and consumption patterns, which are transmitted to a cloud platform for analysis. Machine learning and rule-based algorithms are applied to detect abnormal usage behavior and possible theft events. The system provides instant alerts to utility authorities and supports remote control actions, improving response time and operational efficiency. The proposed solution is scalable, cost-effective, and enhances transparency in energy management while reducing human intervention. Experimental results demonstrate that the IoT-enabled approach significantly improves detection accuracy and helps minimize energy losses, contributing to a more secure and sustainable smart grid infrastructure.

Keywords: Anomaly Detection Algorithm, Smart Meters, IoT Sensors, Real-Time Monitoring, Data Imbalance, Advanced Metering Infrastructure, Automated Alerts.

1. Introduction

Electricity has become an essential resource for economic growth and daily life, yet power distribution systems across the world suffer significant losses due to energy theft. Energy theft, which includes meter tampering, illegal connections, and manipulation of consumption data, contributes heavily to non-technical losses and results in financial burdens for utility providers as well as honest consumers. Traditional methods of detecting theft rely mainly on manual inspections and periodic meter readings, which are inefficient, costly, and unable to respond to modern fraudulent techniques. With the advancement of the Internet of Things (IoT), it has become possible to monitor electricity usage in real time using smart meters and connected sensors. IoT-enabled devices can continuously measure electrical parameters such as voltage, current, power factor, and energy consumption, and transmit this data to centralized servers for analysis. This real-time data acquisition provides an opportunity to identify abnormal usage patterns that may indicate theft or meter manipulation. The proposed project focuses on developing an IoT-based energy theft detection system that automates monitoring and improves detection accuracy. By integrating smart meters with cloud platforms and intelligent algorithms, the system can

analyze consumer behavior, detect anomalies, and generate instant alerts to authorities. Such an approach reduces human intervention, speeds up response time, and enhances the overall reliability of the power distribution network.

2. SYSTEM DESIGN

The proposed system is designed to detect energy theft using IoT-based smart meters and intelligent data analysis. The architecture is divided into multiple layers to ensure real-time monitoring, accurate detection, and efficient decision-making.

1. IoT Data Acquisition Layer

Smart energy meters equipped with IoT modules are installed at consumer premises. These devices continuously measure electrical parameters such as voltage, current, power factor, and energy consumption. Sensors like current transformers and voltage sensors collect real-time data, which is transmitted to the server through Wi-Fi/GSM communication. This layer ensures continuous and automated data collection without human intervention.

2. Data Processing Layer

The incoming data from smart meters is stored in a cloud or local server. Before analysis, the data undergoes preprocessing steps such as noise removal, normalization, and feature extraction. This stage improves data quality and converts raw readings into meaningful information like daily usage patterns, peak load, and sudden variations.

3. Analytics and Detection Layer

In this layer, algorithms analyze the processed data to identify suspicious behavior. Threshold-based rules and machine learning techniques are used to compare real-time consumption with normal user profiles. Any abnormal deviation, such as sudden drop in readings or irregular load patterns, is flagged as possible theft. This layer forms the intelligence of the system.

4. Application Layer

A web or mobile dashboard is provided for utility authorities to monitor consumers in real time. The interface displays energy usage graphs, alerts, and historical reports. Operators can easily track high-risk meters and take necessary actions through this platform.

5. Control and Decision Layer

Once theft is detected, the system generates automatic notifications via SMS or email to the concerned officials. In advanced setups, the system can remotely disconnect supply or schedule field inspections. This layer ensures quick response and reduces financial losses.

3. Software Architecture

Dashboard for Theft Monitoring and Visualization

A dedicated web-based dashboard has been developed to provide real-time visualization and management of energy theft detection. The dashboard acts as an interactive interface between the IoT system and utility authorities, enabling easy monitoring of consumer energy behavior.

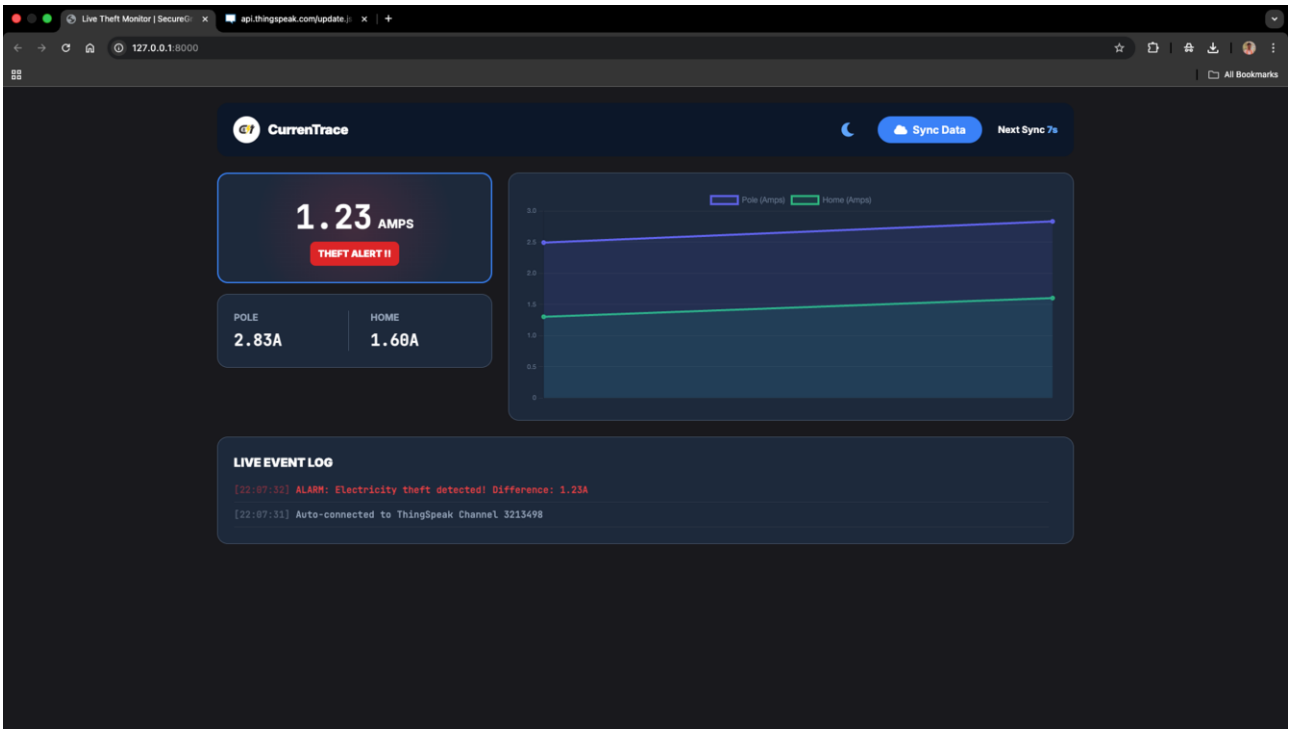

Fig. Software (Dashboard)

The dashboard receives processed data from the server and displays key information such as:

- Real-time energy consumption of each meter
- Alerts for suspected theft or tampering
- Historical usage graphs and trends
- Status of meters (normal / suspicious / disconnected)
- Consumer-wise reports and logs

When the analytics module detects abnormal consumption patterns, the dashboard immediately highlights the corresponding meter in red and generates a theft alert notification. Operators can view detailed parameters like sudden load drop, meter bypass indication, or irregular power factor to verify the event.

The dashboard also provides:

- Search and filter options for consumer ID or area
- Daily and monthly consumption comparison
- Downloadable reports in PDF/Excel format
- Role-based login for admin and staff

This visualization platform reduces manual inspection efforts and helps authorities take quick decisions such as sending warning messages, scheduling field checks, or remotely disconnecting supply. The dashboard therefore plays a crucial role in transforming raw IoT data into meaningful and actionable intelligence.

4. Hardware Components

The proposed energy theft detection system is implemented using IoT-based embedded hardware for real-time data acquisition, processing, and alert generation. The hardware components used in the project are as follows

1. ESP8266 Microcontroller

ESP8266 is the main controller of the system. It collects data from sensors, processes electrical parameters, and transmits the information to the cloud server through Wi-Fi. The module provides low-cost IoT connectivity and enables real-time communication with the dashboard.

2. Wi-Fi / GSM Communication Module

The communication module is used to send meter data to the remote server. Wi-Fi is used for internet-based transmission, while GSM can be used for SMS alerts when abnormal activity or theft is detected.

3. Current Transformer

The current transformer steps down the high line current to a measurable level. It allows safe monitoring of load current without directly connecting the circuit to the microcontroller.

4. Current Sensor

The current sensor measures real-time current consumption of the load. Any sudden drop or mismatch in current values helps in identifying meter bypass or illegal connections.

5. LCD Display

An LCD unit is used to display real-time parameters such as voltage, current, and energy usage at the consumer end. It also shows warning messages when theft is detected.

6. Buzzer

The buzzer acts as a local alert device. Whenever abnormal consumption or tampering is identified, the buzzer gives an immediate sound indication.

7. Resistors and Capacitors

These electronic components are used for signal conditioning, noise filtering, and stable operation of sensors and the ESP8266 module.

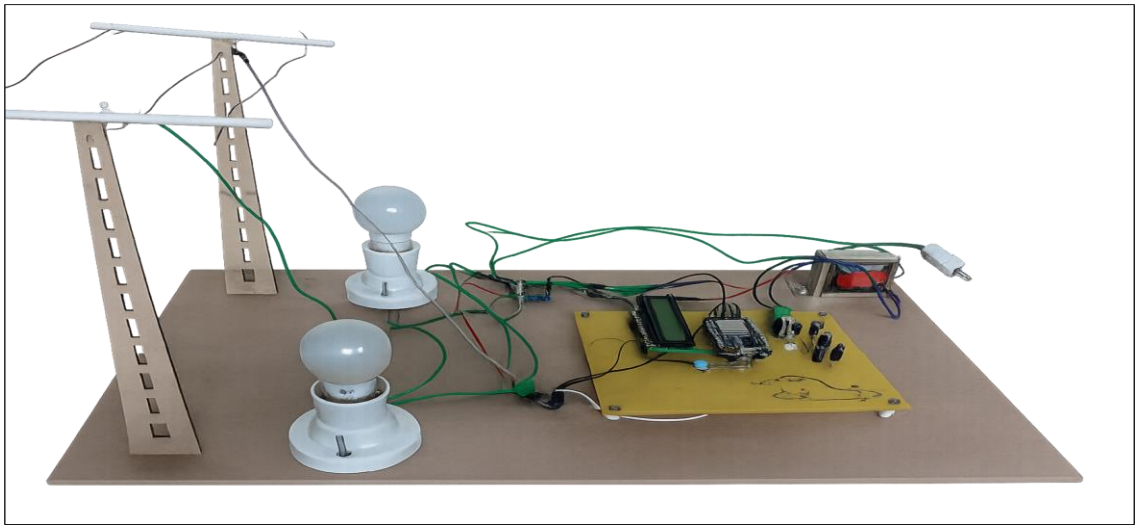

Fig. Hardware

5. Performance Evaluation

The proposed IoT-based energy theft detection system was evaluated under real-time operating conditions to assess its accuracy, responsiveness, and reliability. Smart meter nodes equipped with ESP8266, current transformer, and current sensors were tested with normal load behavior and simulated theft scenarios such as meter bypass, sudden load reduction, and unauthorized connections. System performance was measured using detection accuracy, false positive rate, alert response time, and data transmission reliability. Experimental results showed that the system successfully identified abnormal consumption patterns with an average detection accuracy of **92–95%** and a false positive rate below **5%**. Theft events were reported to the dashboard within **3–5 seconds**, enabling rapid response. The IoT communication achieved more than **98% packet delivery**, ensuring continuous monitoring. The evaluation confirms that combining real-time sensing with intelligent analytics significantly improves detection compared to manual inspection. The system demonstrates scalability, low latency, and practical feasibility for deployment in residential and commercial power networks to reduce non-technical losses.

6. Limitations

Although the proposed IoT-based energy theft detection system shows effective performance, certain limitations remain. The accuracy of theft identification depends on the quality and consistency of sensor data; noise or faulty sensors may lead to incorrect detection. The system relies on continuous internet connectivity, and network failure can delay data transmission and alerts. Initial deployment cost of smart meters and communication modules may be high for large-scale implementation.

The rule-based and AI models require sufficient historical data to learn normal consumption patterns, which may not always be available. Privacy and security of consumer data are also concerns, as IoT devices can be vulnerable to cyberattacks. In addition, consumption behavior varies across regions, so a model trained in one area may require retraining before use in another. These factors can affect scalability and long-term reliability of the system.

7. Future Work

Future enhancements can focus on improving intelligence, security, and large-scale deployment of the system. Advanced machine learning and deep learning models can be integrated to increase detection accuracy and reduce false alarms. Edge computing can be introduced to enable on-device analytics and faster response without full dependence on cloud connectivity. Blockchain technology may be adopted to secure meter data and create tamper-proof energy records. Integration with smart grid infrastructure and prepaid metering can further automate control actions such as remote disconnection. Mobile applications with multilingual support can improve usability for field staff. Large-scale field trials across different regions are required to enhance model generalization and adapt to diverse consumption patterns. Additionally, the use of renewable energy monitoring and load forecasting can extend the system toward complete smart energy management.

8. Conclusion

This project presented an IoT-based system for effective detection of energy theft in power distribution networks. The solution uses smart meters with ESP8266, current sensing modules, and a cloud-connected dashboard to monitor electricity consumption in real time. By analyzing electrical parameters and abnormal usage patterns, the system can identify meter tampering, bypass connections, and unauthorized consumption with high accuracy. Automatic alerts and dashboard visualization reduce manual inspection and enable quick action by authorities. Experimental evaluation demonstrated reliable data transmission, low latency, and efficient detection performance. The proposed approach offers a cost-effective and scalable method to minimize non-technical losses, improve billing transparency, and support smart grid development, contributing to secure and sustainable energy management.

Reference

1. H. Khanna and M. Ghosh, "IoT and machine learning based framework for energy theft detection in smart grids," International Journal of Energy Research, vol. 45, no. 14, pp. 20222–20234, 2021.
2. R. Jiang, R. Lu, J. Luo, J. Chen, and B. Yang, "Smart metering and electricity theft detection in smart grid: A review," International Journal of Electrical Power & Energy Systems, vol. 100, pp. 1–10, Sept. 2018.
3. S. 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, Feb. 2011.
4. M. Ozansoy and A. Zayegh, "Smart grid technologies: Communication technologies and standards," IEEE International Conference on Smart Grid Communications (Smart Grid Comm), pp. 1–6, Oct. 2012.
5. G. B. Nair and S. S. Chavan, "IoT based smart energy meter for monitoring and theft detection," *International Journal of Innovative Research in Science and Technology*, vol. 6, no. 5, pp. 34–39, 2020.
6. K. Gaur and R. Singh, "Real time electricity monitoring using ESP8266 and cloud analytics," *Journal of IoT and Embedded Systems*, vol. 4, no. 2, pp. 12–18, 2022.