

Review on Energy Theft Detection Using AI and IOT

Tejas Nandan¹ Nishant Khule² Harshal Mali³ Sakshi Adole⁴ Mr. Chandrakant Aher⁵

^{1,2,3,4}Student ⁵Lecturer

^{1,2,3,4,5}Department of Information Technology

^{1,2,3,4,5}Rajarshi Shahu Maharaj Polytechnic, Nashik, Maharashtra, India

Abstract — Energy theft is a big problem that leads to financial losses and weakens the stability of power distribution systems. Traditional ways of detecting theft often don't work well against modern methods like tampering with meters or making illegal connections. To solve this, our work suggests using Artificial Intelligence (AI) and the Internet of Things (IoT). Smart meters and IoT sensors can collect electricity usage data in real time, and machine learning can then analyze this data to spot unusual patterns and possible theft. This system makes theft detection more accurate, allows real-time monitoring, and provides a scalable and affordable way to improve energy security and support sustainable power distribution.

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

I. INTRODUCTION

Energy theft is a serious problem that causes huge financial losses, lowers the efficiency of power grids, and makes electricity bills unfair for honest consumers. Traditional methods of detecting theft often fail, especially against advanced tricks like meter tampering, illegal connections, or manipulating data. To deal with this issue, modern technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT) are proving very useful. Smart meters and IoT sensors can track electricity use in real time across the power network. With the help of AI methods like machine learning and anomaly detection, this data can be analyzed to spot unusual consumption patterns and detect theft more accurately. Combining AI with IoT not only improves detection but also allows real-time monitoring, predictive analysis, and automatic alerts. This makes the system more secure, efficient, and cost-effective, while also helping to reduce energy losses and ensure a more reliable and sustainable power supply.

II. SYSTEM DESIGN

A. IoT and Data Acquisition Layer

Smart meters equipped with IoT modules are deployed at consumer premises to continuously measure parameters such as voltage, current, power factor, and consumption. These meters transmit data securely via communication protocols such as Wi-Fi, GSM, or LoRa to the utility server.

B. Data Processing Layer

The collected data are stored in a cloud or edge computing system. Before analysis, the data go through preprocessing steps like removing noise, normalizing values, and extracting important features to make sure the information is clean and reliable.

C. AI Analytics Layer

Machine learning and deep learning models then analyze the cleaned data to spot unusual behavior. The system compares current usage patterns with normal profiles, and if something looks abnormal, it is flagged as possible theft. Different algorithms like anomaly detection, classification, and clustering are used to improve accuracy.

D. Application-Layer

A web or mobile dashboard shows real-time energy usage, theft alerts, and past reports. This interface helps utility companies easily monitor and manage large networks.

E. Control and Decision Layer

Using the insights from AI, the system sends alerts and notifications to utility staff. In serious cases, it can also take automated actions, like remotely disconnecting the power supply or scheduling field inspections.

III. SOFTWARE ARCHITECTURE

The software architecture of the energy theft detection system is built to handle large amounts of incoming data, provide fast real-time analysis, support offline model training, and ensure secure operations.

A. Data Ingestion and Edge

Smart meters and other IoT sensors send electricity usage data using lightweight communication protocols like MQTT or CoAP.

B. Messaging Layer

A message broker, such as an MQTT broker or Kafka, is used to connect data producers and consumers. It helps manage data flow by providing buffering, routing messages based on topics, and handling sudden bursts of incoming data.

C. Stream Processing and Feature Extraction

A stream processing service, such as Apache Flink, Spark Streaming, or Kafka Streams, handles data in real time. It performs tasks like windowing, extracting features (for example, energy differences, load factor, or harmonic indicators), and adding extra details like customer information. After this, the features are saved in a time-series database, and any suspicious events are sent to the model or alerting systems.

D. Storage

A time-series database (like InfluxDB or TimescaleDB) stores high-resolution telemetry and extracted features for quick queries and dashboards. At the same time, a data lake or object storage (such as S3) keeps both raw and processed data for model training and auditing.

E. Model Training and Feature Store

Offline machine learning and deep learning pipelines use historical data to train and test models, including supervised classifiers, autoencoders, and LSTM-based sequence models. A feature store is used to keep feature definitions consistent and versioned. Model artifacts and metadata are also tracked and versioned with tools like MLflow or DVC.

F. Model Serving and Real-time Scoring

Deployed models are hosted in a model server (TF-Serving, Torch-Serve, or containerized REST/gRPC endpoints) for low-latency inference. The stream processor or an API gateway invokes models to score incoming data and emit theft probabilities or anomaly scores.

G. API Gateway, Dashboard and Operations

Once trained, the models are deployed on a model server (e.g., TF-Serving, TorchServe, or containerized REST/gRPC endpoints) for fast, real-time predictions. The stream processor or API gateway calls these models to analyze incoming data and generate theft probabilities or anomaly scores.

H. Monitoring, Security and Governance

The system uses centralized logging, performance metrics, identity and access management (IAM), TLS encryption, and audit trails to make sure everything is observable and compliant. Security is strengthened through role-based access control, data encryption (both during transfer and storage), and anomaly audits. These measures help prevent misuse and support forensic analysis when needed.

I. Scalability And Fault Tolerance

The architecture is designed to scale horizontally using broker clusters, stateless processing, and autoscaling model pods. It also includes fail-safe mechanisms like edge detection and retries queues to handle errors. Data storage policies and model retraining schedules can be adjusted based on the service-level agreements (SLAs) of the utility provider.

1) Anomaly Detection Algorithm

In this system, anomaly detection for energy theft combines real-time monitoring with machine learning to spot unusual electricity usage. Smart IoT meters collect continuous data on factors like energy consumption, voltage, and current. This data is then cleaned and converted into useful features, such as load variations and daily usage patterns. AI models—often unsupervised ones like Isolation Forest, Autoencoders, or time-series models such as LSTM—are trained to learn what normal consumption looks like. Any abnormal deviations from this baseline are flagged as possible theft. Once an anomaly is detected, alerts are sent to utility operators for further checks or automated actions. This makes the detection process faster, more accurate, and less dependent on manual inspections.

2) Classification Algorithm

Classification algorithms are supervised learning methods used to detect energy theft by labeling electricity usage as either “normal” or “fraudulent.” Smart IoT meters collect real-time consumption data, which is then cleaned and converted into features such as average load, peak usage, and

voltage irregularities. Using labeled historical data where both normal and theft cases are already known algorithms like Decision Trees, Random Forests, or Support Vector Machines (SVM) are trained to recognize patterns. After training, the model can classify new usage data in real time, helping utility companies quickly identify and respond to suspicious activity.

IV. HARDWARE COMPONENTS

A. Smart Energy Meters:

Smart energy meters, such as Arduino-based or ESP32-based devices, are used to measure real-time electricity consumption. These meters can also detect irregular activities like tampering or unauthorized usage. (Source: Nevon Projects)



B. Microcontrollers:

Arduino Uno, ESP32, or Atmega328P microcontrollers process data from sensors and manage communication with other system components.

C. Current and Voltage Sensors:

Sensors like ACS712 (current sensor) and ZMPT101B (voltage sensor) monitor electrical parameters to detect discrepancies indicative of theft. SpringerLink

D. Wireless Communication Modules:

Wi-Fi modules (e.g., ESP8266, ESP32) and GSM modules enable remote data transmission and alert notifications. Nevon Projects.

E. Display Units:

LCDs or OLED displays provide real-time feedback to users and maintenance personnel.

F. Power Supply Units:

AC-DC adapters or battery packs ensure continuous operation of the system components.

V. PERFORMANCE EVALUATION

Performance evaluation for energy theft detection with AI and IoT checks how well the system can identify fraudulent electricity use while keeping false alarms low. Typically, historical data from IoT meters are split into training and testing sets. AI models—like supervised classifiers or unsupervised anomaly detectors—are trained on the training

set and tested on unseen data. Important metrics include accuracy, precision, recall, F1-score, ROC-AUC, and false positive/negative rates. These metrics help measure how effectively the system flags theft without overwhelming operators with false alerts. Other important considerations include handling imbalanced datasets, considering time-based usage patterns, adjusting thresholds for anomaly detection, and continuously monitoring performance in real-time to ensure the system remains scalable and reliable.

VI. LIMITATIONS

Even with AI and IoT, energy theft detection faces some challenges. The accuracy of AI models depends on having high-quality and balanced datasets, which are not always available. Deploying IoT devices on a large scale can be expensive and requires proper infrastructure and skilled maintenance. Privacy and security are also concerns because continuous monitoring can expose sensitive data, and IoT devices may be vulnerable to cyberattacks. Additionally, models trained for one region may not work well in areas with different consumption patterns. These issues can limit the system's scalability and long-term effectiveness.

VII. FUTURE WORK

Future research can focus on making AI and IoT-based energy theft detection systems more robust and scalable. Techniques like federated learning and edge AI could reduce reliance on centralized data while protecting privacy. Lightweight anomaly detection algorithms can be designed for resource-limited IoT devices, enabling faster real-time analysis. Blockchain technology may also be used to secure data exchange and create tamper-proof billing records. Furthermore, conducting large-scale field trials across different regions is important to improve model generalization and test the system's effectiveness in real-world conditions.

VIII. CONCLUSION

This work presented an AI and IoT-based system for detecting energy theft in power distribution networks. By using smart meters to collect real-time data and applying AI for anomaly detection, the system can identify theft more accurately and respond faster than traditional methods. Its layered architecture supports scalability, real-time monitoring, and decision-making for utility companies. While challenges like data quality, security, and deployment costs remain, this approach shows strong potential to reduce non-technical losses, improve grid reliability, and promote 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.