ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1177

IoT and ML Based Electricity Theft Detection

Obbu Chandra Sekhar[1]; Aakashdeep[2]; Arnav Tyagi[3]; Gaurav Kumar[4]

[1,2,3,4] Electrical Engineering Department, National Institute of Technology, Delhi

Publication Date: 2025/05/23

Abstract: Electricity theft continues to be a major concern in the power sector, leading to significant financial and operational setbacks. This paper presents an Internet of Things (IoT)-based electricity theft detection system en- hanced with machine learning capabilities. Smart energy meters equipped with sensors, microcontrollers, and wireless communication modules are deployed to monitor real-time power consumption. The collected data is transmitted to a cloud-based platform, where it is used to train a machine learning model for accurate anomaly detection. By learning typical usage patterns, the model improves the precision and reliability of theft identification. Upon detecting irregularities such as tam-pering or unauthorized usage, the system generates auto- mated alerts and enables remote intervention by authorized personnel. This approach enhances grid security, supports proactive loss prevention, and lays the ground- work for scalable, data-driven energy management. Fu- ture work includes the integration of blockchain for data integrity and further system resilience.

How to Cite: Obbu Chandra Sekhar; Aakashdeep; Arnav Tyagi; Gaurav Kumar. (2025) IoT and ML Based Electricity Theft Detection. International Journal of Innovative Science and Research Technology, 10(5), 1219-1224. https://doi.org/10.38124/ijisrt/25may1177

I. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative technology, enabling seamless connectivity and data exchange between physical devices through the internet. In the energy sector, IoT facilitates smarter monitoring, control, and manage- ment of power systems. Despite these advancements, electricity theft remains a persistent issue, leading to financial losses, oper- ational inefficiencies, and safety concerns. Traditional detection methods are often reactive, inaccurate, and resource-intensive. This study introduces an IoT-based electricity theft detection system integrated with machine learning to enhance accuracy and responsiveness. Smart meters equipped with sensors and wireless modules collect real-time consumption data, which is analyzed for anomalies using trained models. The system offers immediate alerts and remote intervention capabilities, promot- ing secure, transparent, and efficient energy distribution. *Figure 1 shows the block diagram of the model.

II. PROBLEM STATEMENT

Electricity theft is a widespread and persistent issue that under- mines the financial and operational stability of power utilities. Common practices such as meter tampering, illegal tapping, and bypassing not only cause significant revenue losses but also compromise grid efficiency and safety. Existing theft detection methods are largely manual, time-consuming, and ineffective in identifying unauthorized usage in real time. This lack of timely detection leads to delayed intervention, higher operational costs, and reduced consumer trust. Moreover, in many developing regions, a substantial portion of transmission and distribution losses is directly linked to non-technical factors like theft. Addressing this challenge requires a scalable, intelligent, and automated system capable of real-time monitoring and ac- curate anomaly detection to ensure secure and efficient power distribution.

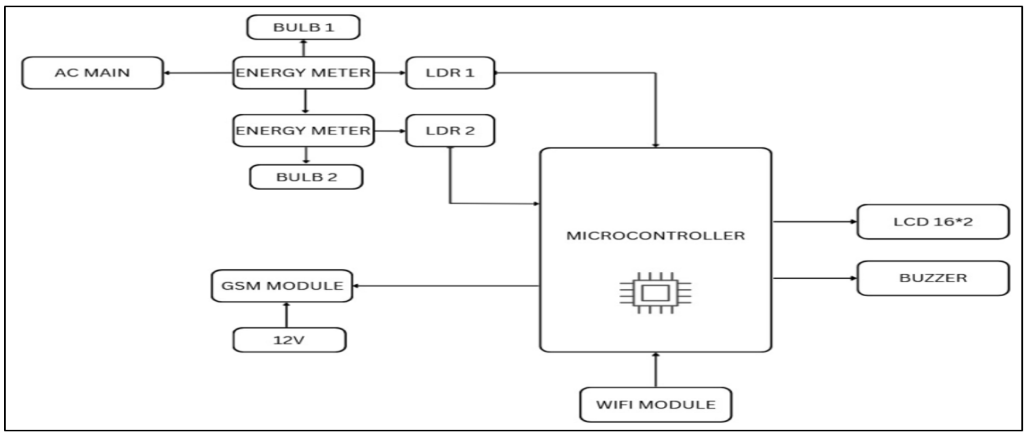

Fig 1 Block Diagram of IoT Model used.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1177

III. LITERATURE REVIEW

Previous studies have explored various techniques to combat electricity theft, ranging from hardware-based tamper detection to software-driven anomaly analysis. Many researchers have implemented smart meters and wireless sensor networks for real-time monitoring of energy consumption. Others have applied machine learning models, such as decision trees and neural networks, to detect abnormal usage patterns. However, these approaches often face limitations in scalability, cost, or real-time responsiveness. Integrating IoT with machine learning presents a promising direction by enabling continuous data collection, cloud-based processing, and accurate theft detection. This hy- brid approach enhances system efficiency while addressing the shortcomings of earlier methods.

IV. COMPONENTS USED

The proposed system integrates both hardware and software components to achieve real-time electricity theft detection. The key components used are as follows:

A. Arduino (Microcontroller)

A low-cost Wi-Fi enabled microcontroller (using Wi-Fi module) that serves as the central processing unit. It collects sensor data and transmits it to the cloud for analysis. (Fig. 2)

Fig 2 Block Diagram of IoT Model used

B. Electricity Meter

Measures total energy consumption over time and serves as the baseline to detect discrepancies or unauthorized usage. (Fig. 3)

C. LCD (16x2 Display)

Used to display real-time consumption data and system status locally. (Fig. 4)

D. GSM Module

Facilitates wireless communication by sending alert messages to authorities in the event of detected anomalies or theft. (Fig. 5)

Fig 3 Electricity Meter

Fig 4 LCD (16x2 display)

Fig 5 GSM Module

E. IoT Platform (ThingSpeak)

A cloud-based dashboard for real-time monitoring, data visual- ization, and alert management. (Fig. 6)

Fig 6 IoT Platform (ThingSpeak)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1177

F. Machine Learning Environment

Used for training and deploying the theft detection model based on consumption patterns.

V. MODELING AND ANALYSIS ON THINGSPEAK

In the proposed system, ThingSpeak is used as the cloud-based IoT platform for data visualization, storage, and analysis of real-time electrical parameters. The NodeMCU microcontroller collects data from current and voltage sensors, which is then transmitted to ThingSpeak via Wi-Fi. The platform displays real-time graphs for voltage, current, and calculated power con- sumption, allowing both utility providers and users to monitor energy usage remotely. Each parameter is assigned to a separate field on the ThingSpeak channel, ensuring clear and structured data presentation. The visualized trends help identify abnormal consumption patterns, which may indicate possible theft. ThingSpeak also supports integration with MATLAB for further data analysis, enabling the implementation of logic to trigger alerts when thresholds are exceeded. This cloud-based monitoring not only facilitates accurate detection but also enhances transparency and responsiveness in managing electricity distribution. Fig. 7 shows the full setup of the IoT Model showing the bulbs lightened.

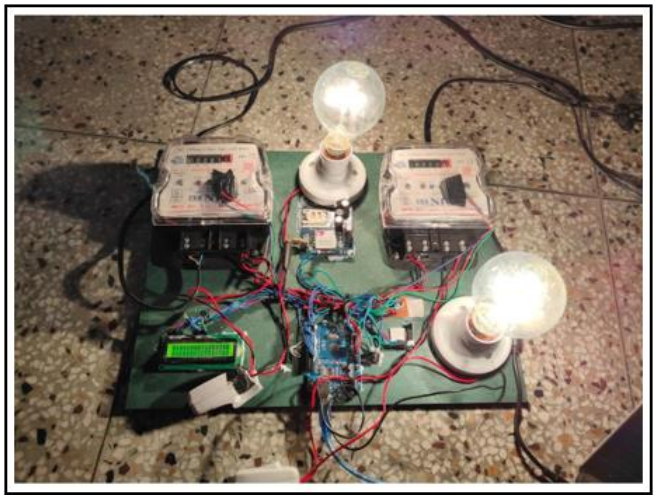

Fig 7 Full Setup of IoT Model

VI. ALGORITHM FOR ARDUINO CODE

A. Step-by-step Algorithm for IoT based Electricity Theft Detection using Arduino UNO is as follows:

- Initial Setup: When the Arduino turns on, first set up the display and communication. Initialize the LCD screen so it can show text messages. Also start serial communication between the Arduino and the ESP8266 Wi-Fi module. This prepares the devices so they can talk to each other and to the LCD.
- Connect to Wi-Fi: Next, use the ESP8266 module to join the home or office Wi-Fi network. The Arduino provides the network name (SSID) and password to the ESP8266, which attempts to connect. Wait until a connection is made. (The ESP8266 is a small Wi-Fi board that gives the Arduino internet access.)
- Monitor Sensors (Main Loop): Enter the main loop of the program, which runs over and over. Inside this loop, read analog input values from the two sensors connected to pins A4 and A5 on the Arduino. These sensors simulate electricity usage at Point 1 and Point 2. For example, a higher analog reading means higher usage and a lower reading means less usage.
- Increment Counters: For each sensor(Point 1 and Point 2), check if the reading is below a set threshold. (The threshold is a chosen value that defines what counts as "low usage.") If a sensor's value is below the threshold, it means an unusual drop in that point's usage is detected. In that case, increase that point's counter by one. Each point has its own counter that tracks how many times the reading was low.
- Detect Possible Theft: Compare the two counters. If one counter is greater than the other by more than a defined margin (a set difference value), this signals a possible theft. In other words, one point has recorded many more low-usage events than the other. This imbalance suggests someone might be drawing power without it being counted at one point.
- Raise an Alert: If the check finds a possible theft, take action immediately. Turn on the buzzer to make a loud sound and also use the serial link to send an alert message (like an SMS) to the user. The Arduino can write a message such as "Theft Detected!" over the serial connection. On the LCD you might also display a warning message. This alerts people nearby and any remote monitor that something is wrong.
- Send Data to ThingSpeak: Continuously, the Arduino sends data to the ThingSpeak cloud platform via the ESP8266. It sends three kinds of data at different intervals:

- Every 6 seconds, send the counter value for Point 1.
- Every 15 seconds, send the counter for Point 2.
- Every 26 seconds, send the theft alert status (for example, "1" if theft was detected, or "0" otherwise).

VII. RESULT & ANALYSIS

The data is continuously recorded and stored in a remotely connected database. The retrieved records from this database are displayed below. Fig 8 and Fig 9 shows the graph which presents the comparative readings from multiple meters as logged on Thing Speak, helping detect inconsistencies over time. To ensure timely response and effective communication in the event of electricity theft or irregular power consumption, the system incorporates a GSM (Global System for Mobile Communications) module interfaced with the Arduino microcontroller. Upon detection of unauthorized electricity usage, the Arduino processes the data received from the energy meter and initiates a predefined response through the GSM module. This response involves the automatic transmission of SMS alerts to both the electricity service provider and the suspected user involved in the anomaly.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1177

Fig 8 Readings of both meters in a specific time interval from Thing Speak Cloud

Fig 9 Readings of both meters in a specific time interval from Thing Speak Cloud

The notification contains essential details regard- ing the incident, enabling immediate attention and action. This mechanism not only enhances the system's responsiveness but also contributes to the transparency and accountability of the power distribution process. A screenshot of the SMS alert, as received by the concerned recipients, is presented below for reference. Fig. 10 shows an example of an alert SMS sent by the GSM module to the concerned party, notifying them of suspicious power consumption behavior.

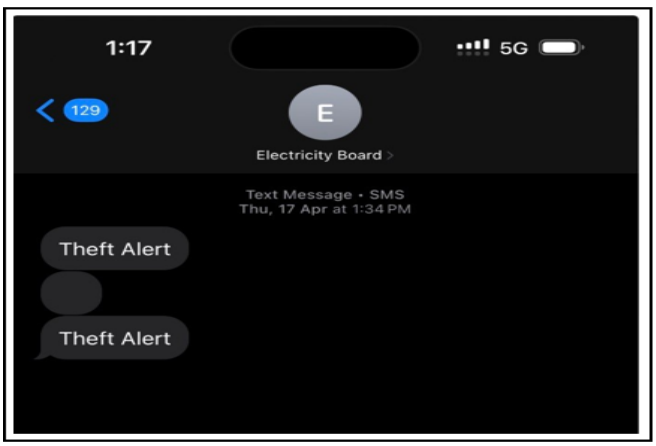

Fig 10 Message Received on Mobile Phone upon Theft Detection

VIII. MACHINE LEARNING INTEGRATION

To strengthen the robustness and scalability of the proposed elec- tricity theft detection system, a machine learning (ML) module was incorporated to enable intelligent analysis of consumption behavior. This addition aims to equip the system with the ability to autonomously learn patterns in energy usage and identify deviations that may indicate potential theft. Initially, data collected through the IoT setup on the ThingSpeak platform was limited in scope and variation, rendering it insufficient for train- ing an effective ML model. To address this limitation, a publicly available dataset comprising extensive smart meter readings from a diverse user base was utilized. This dataset offered the granularity and labeled instances necessary for reliable training and testing of supervised learning algorithms. A classification model was developed to distinguish between normal and anomalous usage patterns. While the current focus remains on refining the model using the external dataset, plans are in place to integrate the validated ML model with the real-time data pipeline of the custom IoT infrastructure in a subsequent development phase. This integration will enable live anomaly detection and automated alerting based on actual consumption behavior.

IX. ALGORITHM FOR TRAINING AND USING ML MODEL

A. Data Generation and Preprocessing

- Simulate a dataset representing electricity usage with mul- tiple contextual features.
- Encode categorical variables (e.g., customer type, region) using one-hot encoding.
- Inject synthetic theft patterns by randomly modifying selected consumption-related parameters to simulate abnor- mal behavior.
- Label data instances as either theft (1) or non-theft (0).

B. Model Training

- Separate the dataset into training and testing subsets.
- Train a supervised classifier (Random Forest) to learn the distinction between normal and theft-labeled consumption patterns.
- Calculate and store feature importance scores for later interpretation.

C. Theft Detection

- Apply the trained model to new data.
- Predict binary labels indicating the presence or absence of electricity theft.
- Store flagged instances for further inspection and alert gen- eration.

D. Anomaly Detection (Unsupervised)

- Employ an Isolation Forest algorithm to independently de- tect consumption anomalies based on learned distribution.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1177

- Assign an anomaly score to each instance and isolate outliers.

E. Data Visualization

- Plot and analyze the distribution of energy consumption across the dataset.
- Highlight central tendencies such as mean usage.

F. Real-time Simulation

- Stream data instances iteratively to simulate real-time usage monitoring.
- For each incoming data point, perform immediate theft prediction.
- Log detection outcomes with corresponding customer identifiers.

G. Explainability (XAI Component)

- Extract and display the top features contributing to the model's decisions.
- Support human interpretation by visualizing feature importance rankings.

X. RESULTS & ANALYSIS FROM ML MODEL

The implemented machine learning framework, utilizing a Ran- dom Forest classifier, demonstrated robust performance in distinguishing between legitimate and suspicious electricity con- sumption patterns. As evidenced by the confusion matrix and classification metrics, the model achieved high predictive ac- curacy with a notably low rate of false positives—an essential attribute for minimizing unwarranted alerts in practical applications.

To evaluate real-world applicability, a simulated real-time data stream was executed. The model successfully processed sequential input and generated timely alerts for anomalous con- sumption events. This responsiveness highlights the frame- work's potential for integration into IoT-enabled smart grid in- frastructures, where prompt detection is critical for operational efficiency and loss mitigation.

Fig 11 Theft Testing using ML Model

Fig 12 Important Factors

An analysis of feature importance, presented in Figure 12, identified power factor, consumption, and voltage as the most influential variables in detecting electricity theft. These results are consistent with domain-specific expectations, where irregu- larities in power factor and voltage often signal unauthorized activity. Additionally, the consumption distribution visualiza- tion (Figure 13) showed a predominantly normal usage pattern among consumers, with theft instances manifesting as statistical outliers. This behavior validates the anomaly-based approach adopted in the study and reinforces the interpretability of the model.

The insights gained from this analysis not only enhance the transparency of the detection process but also offer practical guidance for optimizing future sensor deployments and prioritizing data streams within IoT frameworks. Fig. 12 presents the analysis of feature importance showcasing the top variables such as power factor and consumption that influence theft prediction. Fig. 13 represents the graph which ranks input features based on their impact on the ML model's decision-making process, aiding explainability.

XI. CONCLUSION

This project presents the successful development and deploy- ment of an IoT-based, cloud-connected electricity theft detec- tion and monitoring system. The proposed architecture seam- lessly integrates both hardware and software elements to pro- vide an autonomous solution capable of identifying and record- ing unauthorized energy usage without requiring manual over- sight. Through the use of embedded sensors and a cloud-based dashboard, the system continuously captures power metrics and stores them on the ThingSpeak platform, enabling remote access and real-time data analysis. One of the core advancements introduced in this work is the incorporation of a machine learning (ML) module to enhance theft detection capabilities. Since the initial IoT dataset was relatively limited, a larger syn- thetic dataset was generated to train and validate a supervised Random Forest classifier. The model demonstrated high per- formance in distinguishing fraudulent from normal consump- tion patterns, as supported by evaluation metrics and visual- ization of feature importances. Notably, parameters such as power factor and overall consumption were found to have the strongest influence on prediction outcomes. This analytical layer not only strengthens detection accuracy but also provides inter- pretability through explainable AI techniques, guiding future improvements in deployment and sensor configuration. Overall, the system contributes to addressing a

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1177

long-standing challenge in power distribution—electricity theft—by offering a scalable, data-driven approach. Beyond identifying theft, the captured and analyzed consumption data can help utility providers optimize infrastructure, detect early signs of faults, and enhance energy planning. This fusion of IoT with intelligent analytics paves the way for more secure, transparent, and efficient energy networks. The results from this project affirm the value of lever- aging modern technologies in critical infrastructure, and sug- gest promising avenues for future expansion using real-world datasets and more advanced ML models.

REFERENCES

[1]. A. A. K. Gupta, A. Mukherjee, A. Routray and R. Biswas, A novel power theft detection algorithmfor low voltage distribution network , IECON2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, 2017, pp. 3603-3608.
[2]. M. Golden, B. Min, Theft and loss of electricityin an Indian Statetechnical report, Int. Growth Centre 2012.
[3]. Navani JP, Sharma NK and Sapra S. Technical and non-technical losses in power system and its economic consequence in Indian economy, Int JElectron Comp Sci Eng, Vol 1, pp. 757–61, 2012.
[4]. W. Han and Y. Xiao, NFD: A practical scheme to detect non-technical loss fraud in smart grid, 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp.605-609.
[5]. ECI Telecom Ltd., Fighting Electricity Theft with Advanced Metering Infrastructure (March 2011) [Online] Available: http://www.ecitele.com
[6]. Kang, B., Lee, J., & Hur, H. (2016). Electricity theft detection using AMI data. 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), 2016. DOI: 10.1109/ APPEEC.2016.7779560
[7]. J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and M. Mohamad, Nontechnical Loss Detection for Metered Customers in Power Utility UsingSupport Vector Machines, in IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162-1171,April 2010.
[8]. S.S.S.R. Depuru, Modeling, Detection, and Prevention of Electricity Theft for Enhanced Performance and Security of Power Grid, The University of Toledo, Aug. 2012.
[9]. J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed, and A.M. Mohammad, Detection of abnormalities and electricity theft using genetic support vector machines, Proc. IEEE Region 10 Conference TENCON, Hyderabad, India, Jan. 2009, pp. 1–6
[10]. S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, Electricity theft detection using smart meter data, in Innovative Smart Grid Technologies Conference (ISGT), IEEE Power and Energy Society, 2015.