IOT based smart energy meter monitoring with theft detection

Vinitkumar V. Patel[1], Saurabh S. Desale[2], Prachi D. Patil[3] and Pratiksha K. Patil[4]

[1] *Assistant professor, Department of Electronics and Telecommunication Engineering, R. C. Patel Institute of Technology, Shirpur, Maharashtra, 425405, India*

[2,3,4] *UG-Students, Department of Electronics and Telecommunication Engineering, R. C. Patel Institute of Technology, Shirpur, Maharashtra, 425405, India*

***Abstract*—Smarter energy management solutions are needed due to the increasing demand for electricity, rising cases of power theft, and inefficiencies in traditional metering systems. The IoT- based Smart Energy Meter Monitoring System with Theft Detec- tion developed in this project aims to provide accurate billing, real-time monitoring, and improved protection against energy theft. The system uses an electronic energy meter connected to an Arduino Uno, which continuously measures electrical parameters such as voltage, current, and power usage. The measured data is displayed locally on an LCD screen and can also be transmitted for remote monitoring. By observing unusual usage patterns or unauthorized changes in load conditions, the system can detect possible theft. When suspicious activity or excessive consumption is identified, a buzzer alerts the user immediately. This solution reduces billing errors, minimizes the need for manual meter readings, enhances transparency for consumers, and helps utility companies prevent losses caused by energy theft.**

I. INTRODUCTION

Electric energy is one of the most crucial resources for economic and social progress. Conventional energy meters are difficult to read by hand, prone to error, and vulnerable to electricity theft. Power theft causes utility companies to suffer significant financial losses, which further burdens reliable cus- tomers. Additionally, because standard meters do not provide real-time usage data, energy management is difficult for both customers and service providers. The Internet of Things (IoT) has enabled intelligent energy meters with automated billing, remote access, and real-time monitoring. By integrating em- bedded systems, sensors, and communication technologies, smart meters improve efficiency, accuracy, and security. The project's objective is to develop an Internet of Things (IoT)- based smart energy meter that monitors energy consumption and searches for anomalous usage patterns that could indicate theft.

II. OBJECTIVES

1) Create and implement an IoT-based smart energy meter: Create a dependable and affordable smart meter system
that uses IoT connectivity to gather and handle energy data from a distance.
2) Enable real-time monitoring of electricity consump- tion: Give utility operators and end users continuous, real-time tracking and visualization of electricity consumption so they can quickly identify usage trends.
3) Identify abnormal usage and power theft: To quickly identify possible electricity theft, use analytics and threshold- based alerts to spot irregular consumption patterns.
4) Automate meter reading and billing: By securely cre- ating billing data via remote communication and automatically gathering meter readings, you can minimize manual labor.
5) Boost energy efficiency and transparency: Provide consumers with clear information about how much energy they use, and produce reports that promote economic electricity consumption and aid in improved demand management.

III. LITERATURE SURVEY

Many academics have proposed smart metering systems us- ing GSM, RF, and IoT technologies. Early systems employed GSM-based SMS transmission, which had limited data rates and higher operational costs. IoT solutions based on Wi-Fi and NB-IoT offer improved scalability and continuous data availability. An earlier study found that current sensor-based theft detection is effective in identifying illegal tapping and meter bypass. However, many systems lack cloud integration and real-time alert systems. Some advanced techniques for anomaly detection involve machine learning, however doing so increases the system's complexity and expense. By utilizing sensor comparison techniques with IoT cloud connectivity, the suggested solution combines a simplicity, affordability, and accuracy, making it appropri ate for modest business and domestic applications.

IV. SYSTEM ARCHITECTURE

1. AC Main Supply: The AC main supply serves as the system's principal electrical power source, supplying all associated

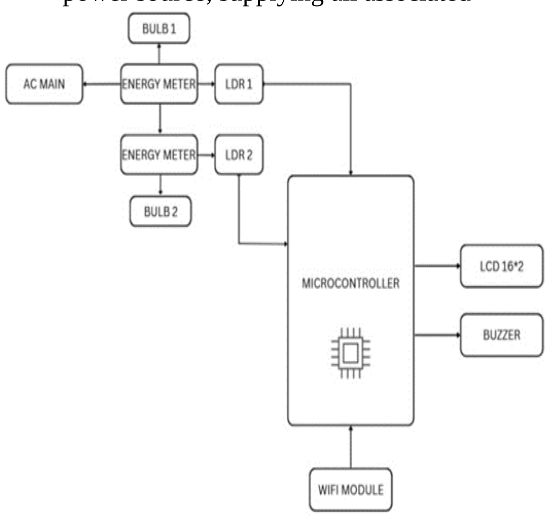


Fig. 1. Block Diagram

loads such as appliances, sensors, and control devices with the energy they require. It also acts as the energy meter's input, allowing precise electricity consumption measurement. Because any unauthorized tapping, bypassing, or tampering might lead to electricity theft and erroneous readings, it is crucial to keep an eye on the AC main.

2. En`ergy Meter: The electrical energy used by linked loads, like Bulb 1 and Bulb 2, is measured by the energy meter. It transforms electrical characteristics, such as voltage and current, into quantifiable values, usually kilowatt-hours (kWh). Within this system, the microcontroller receives real- time usage statistics from the meter. Theft or tampering may be indicated by any disparity between meter readings and actual energy consumption.

Load (Bulb 1 and Bulb 2): Here, bulbs 1 and 2 serve as examples of normal consumer electrical loads for testing and demonstration. Electricity passes via the energy meter during regular operation before it reaches these loads. The system's sensors can identify anomalous conditions created when electricity is unlawfully drawn, circumventing the meter. LDR Sensors (LDR 1 and LDR 2): Light Dependent Resistors (LDRs) serve as sensors for detecting theft and tampering. They pick up on variations in light intensity, which can happen when the meter casing is unsealed or when unapproved bypass wiring is put in. Different parts of the meter or distinct load routes are monitored by LDR 1 and LDR 2. Any abrupt or strange variations in light levels are

regarded as possible attempts at theft or tampering.

Microcontroller: As the system's core control unit, the microcontroller oversees all aspects of its operation. It detects anomalies by comparing actual consumption patterns with typical usage after reading data from the energy meter and LDR sensors. The microcontroller is in charge of operating output devices including the LCD display and buzzer as well as detecting theft conditions like bypassing, meter tampering, or unauthorized access. It also uses the Wi-Fi module to send warning and energy usage data to the cloud, allowing for

V. REMOTE MONITORING

Wi-Fi Module: By sending data to a web dashboard or cloud server, the Wi-Fi module enables the system's Internet of Things features. It enables remote monitoring of real- time energy consumption data and promptly issues alarms in the event of theft or unusual usage. Utility authorities or users can monitor consumption using this capability instead of depending on human meter readings.

LCD Display (16×2): A local visual interface is provided by the 16x2 LCD display, which shows linked loads' energy usage in real time, the status of theft detection, and system alarms or failure messages.

This guarantees that consumers won't want any extra tools to immediately comprehend the state of the system.

Buzzer: When electrical theft or tampering is detected, the buzzer serves as an instant alert system. By providing an immediate warning at the location, the audio alert deters illicit activities and highlights possible meter tampering.

VI. WORKING PRINCIPLE

A. Principle of Operation

Accurate measurement of electrical energy consumption, real-time data transfer, and clever analysis of power usage trends to spot unusual or illegal consumption form the foundation of an Internet of Things-based smart energy meter monitoring system with theft detection. The system continuously measures electrical parameters from the supply line, such as voltage and current, computes power and energy, and uses Internet of Things technology to send the results to a distant server.

Energy theft can be identified by monitoring abrupt changes, bypass situations, and discrepancies between input and output current levels, or by comparing the actual load current with the anticipated or permitted consumption. The system can initiate precautionary steps, including removing the load through a relay, and automatically create alarms when abnormal behavior is identified. IoT integration improves accuracy, transparency, and security while removing the need for manual meter read- ing through remote monitoring, data logging, visualization, and control.

B. Working of the System

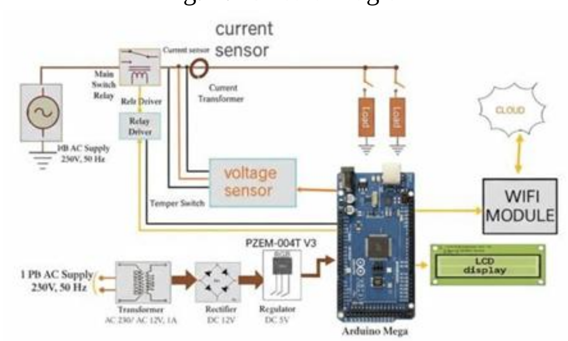
The working of the IoT based smart energy meter mon- itoring with theft detection system can be explained in the following stages:

1. Initialization and Power Supply: A 12V SMPS power supply, which transforms the AC mains voltage into a steady DC voltage, powers the system. In order to provide the microcontroller, sensors, and communication modules with the proper operating voltages (5V or 3.3V), this DC voltage is further regulated using voltage regulators (such as 7805 or buck converters). The microcontroller initializes all attached peripherals, including the display unit, relay, IoT module, voltage sensors, and current sensors, after it is powered up.
2. Energy Measurement: Voltage sensing circuits and cur- rent sensors (such CT sensors or ACS712) are used to measure
3. electrical energy. The consumer's load current is measured by the current sensor, whilst the voltage sensor monitors the line voltage. The microcontroller's ADC pins receive these analog signals. These inputs are used by the microcontroller to compute Instantaneous power, Energy usage (measured in kWh, or kilowatt-hours), Values of load voltage and current. Similar to a traditional energy meter, but with improved accuracy and digital processing, the energy consumption is continually gathered over time.
4. Data Processing and Display: The microcontroller uses embedded algorithms to process the sensor data. For the con sumer's reference, the computed parameters such as voltage, current, power, and total energy consumed are shown locally on an LCD or OLED display. This guarantees openness and enables users to track their energy consumption in real time. 4.IoT-Based Data Transmission: Energy usage data is sent to a cloud server or IoT platform (such as ThingSpeak, Blynk, Firebase, or custom web server) using an IoT communication module such an ESP8266, ESP32, or GSM/GPRS module. Periodically or in real time, the data is uploaded to the internet. This permits the Utility companies' remote energy monitoring, Access to consumption data via online or mobile applications, Keeping track of past usage information forbilling and analysis
5. Theft Detection Mechanism: One important aspect of this system is the detection of energy theft. Theft may result from illicit tapping, meter bypassing, or load manipulation. One or more of the following techniques are used by the system to identify theft: Current mismatch detection: Theft is suspected if the detected current differs from the anticipated consumption pattern. Identification of sudden load variation: Unusual current spikes or decreases suggest potential manipulation. When electricity is extracted without going through the meter sensors, this is known as bypass detection. Unauthorized load connection: When a load above set thresholds. The microcontroller marks the occurrence as energy theft when such anomalous circumstances are found.
6. Alert and Control Action: The system quickly notifies the utility provider or user via the IoT platform when it detects electricity theft. A theft warning message, real-time statistics demonstrating unusual

energy consumption, and identifying information like the location or meter number can all be included in the notifications. To stop additional energy loss, the system can also trigger a relay control mechanism to cut off the power supply to the impacted load in addition to alerting authorities. This disconnection can be managed remotely through the IoT dashboard or automatically by the system, enabling prompt action and improved security.

7. Remote Monitoring and Billing Support: Accurate de- mand forecasting, thorough usage analysis, and automated billing are all made possible by the data kept in the cloud. Customers may easily track how much energy they use on a daily or monthly basis, which helps them control and maximize their use. In the meantime, utility companies can use data analysis to pinpoint regions with high energy losses, spot anomalous consumption trends, and more effectively carry out
corrective actions, enhancing overall system dependability and management.

Fig. 2. Circuit Diagram



C. System Operation

The system is made up of a number of essential parts that cooperate to track energy usage and identify theft. The linked loads are powered by the AC supply, which passes through a relay and current sensor to allow for controlled electrical current delivery and monitoring. Line voltage is measured by a voltage sensor, and real-time voltage, current, power, and energy usage are computed using an Arduino Mega microcontroller. A WiFi module sends data to the cloud for remote monitoring, while a 16x2 LCD display gives local measurements. In order to ensure security and prevent energy loss, the system also includes a theft detecting mechanism that can disconnect the load via the relay and send out alarms.

V. METHODOLOGY

In order to guarantee precise monitoring and prevention of power theft, the methodology of the suggested IoT-based smart energy meter monitoring with theft detection system focuses on the design, implementation, data gathering, communication, and analysis of electrical energy usage. The entire process is broken down into a number of methodical phases, which are explained below. The microcontroller, current sensor, voltage sensor, relay module, WiFi module, display unit, and regulated power supply are among the hardware components that are first chosen for the system's architecture. A step-down transformer and relay are used to connect the AC mains supply with the system, guaranteeing electrical isolation and safety. High voltage AC is transformed into low-voltage DC by the power supply unit, which is necessary for the microcontroller and other electronic parts.

Data collection and energy sensing are done in the next phase. While a voltage sensor is linked across the supply to track line voltage, a current sensor is connected in series with the load to measure the current drawn by the consumer. Analog signals proportional to current electrical parameters are continuously produced by these sensors. The microcon troller's analog-to-digital converter (ADC) pins receive the
analog outputs, allowing for accurate digital representation of voltage and current values. The microcontroller calculates instantaneous power and cumulative energy consumption in kilowatt-hours (kWh) by processing the collected data using inbuilt algorithms. The data on energy use is updated on a regular basis and momentarily saved for later transmission and comparison. For real-time user monitoring, the measured voltage, current, and energy values are simultaneously shown locally on an LCD display.

In order to send processed data to a cloud-based IoT platform, a WiFi module is interfaced with the microcon troller for IoT-based communication. Regular uploads of the energy usage data enable remote monitoring via a mobile or online application. This makes it unnecessary to manually read meters and makes it simple to get past energy usage data for analysis and billing. Current and power consumption patterns are continuously analyzed in order to implement the theft detection system. Real-time sensor data is compared by the system to standard usage patterns and predetermined threshold values. Potential theft possibilities include irregular consumption patterns, unlawful bypass conditions, sudden load changes, and current mismatches. The technology creates an alert message and sends it to the cloud platform for instant notice when theft is discovered.

A relay control system is included as a precaution. The microprocessor triggers the relay to cut off the power supply to the load after verifying theft or unusual circumstances. This guarantees system security and reduces energy loss. The IoT dashboard and LCD both update the event status at the same time. In order to provide a dependable, automated, and intelligent energy monitoring system with efficient theft detection capabilities, the suggested methodology combines sensing, processing, communication, and control.

VI. OUTCOMES AND ANALYSIS

The created system effectively and accurately detected power, voltage, current, and energy consumption (kWh) in real time. By eliminating the requirement for manual meter reading, continuous energy monitoring was accomplished, minimizing human error and intervention. IoT integration made it possible to remotely monitor energy consumption via a cloud platform, where consumption data was kept for automated billing support and historical analysis. Conditions like abrupt load fluctuations, illegal load connections, and current mismatch or bypass attempts were all successfully identified by the system as signs of electricity theft. Instant alarms were produced and shown on the IoT dashboard upon detection, and the relay control mechanism effectively cut off the load to stop additional energy loss. An LCD panel that showed electrical characteristics and system status was used for local monitoring, and the regulated power supply made sure that the entire system operated steadily and dependably. When compared to traditional energy meters, the intro-duction of digital processing and real-time sensing greatly increased measurement accuracy. Reliable performance was
demonstrated by the theft detection algorithm's prompt re- sponse in atypical situations and lack of false alarms during regular operation. Although system performance is dependent on internet availability, IoT-based data transmission made effective real-time monitoring possible. The improvement in understanding consumption trends and the identification of periods of excessive usage was made possible by cloud-based data visualization. Relay-based power cut-off improved system security and helped save energy. The overall architecture is scalable and appropriate for incorporation into applications for smart cities and smart grids. The research verifies that the system is effective, safe, and appropriate for contemporary energy management despite a few minor drawbacks, such as reliance on network availability and the requirement for recurring sensor calibration.

VII. CONCLUSION

The IoT based smart energy meter monitoring with theft detection project successfully demonstrates an efficient and reliable solution for modern energy management. The system overcomes the limitations of conventional energy meters by providing real-time monitoring, automated data transmission, and intelligent theft detection. By integrating current and voltage sensors with a microcontroller and IoT communication module, the system accurately measures electrical parameters such as voltage, current, power, and energy consumption.

One of the major achievements of this project is the effective detection of energy theft. The system continuously analyzes consumption patterns and identifies abnormal conditions such as sudden load variations, unauthorized connections, and cur- rent mismatches. Upon detecting theft, the system generates instant alerts and activates a relay mechanism to disconnect the power supply, thereby preventing further energy loss. This enhances the security and reliability of the power distribution system.

REFERENCES

[1] IoT-Based Smart Energy Meter Monitoring with Theft Detection, *Jour- nalNX*, vol. 10, no. 5, pp. 72–77, 2024.

[2] K. Pramothini, L. Saranya, and R. C. Nishanthini, IoT Based Smart En- ergy Meter with Power Theft Identification, Int. J.

Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 2021.

[3] Smart Energy Meter with Theft Detection, Journal of Punjab Academy of Sciences, vol. 23, 2023.

[4] L. Anbarasu et al., Smart IoT Energy Metering System with Real-Time Theft Detection and Prevention, Journal of Electrical Engineering and Automation, vol. 7, no. 2, pp. 151–162, 2025.

[5] H. S. Chong, IoT-Based Smart Energy Meter Monitoring with Theft Control, Journal of Engineering and Technological Advances, vol. 9, no. 2, 2025.

[6] N. V. Koteswara Rao et al., Smart Energy Meter by Using IoT, Int. J. for Research in Applied Science and Engineering Technology, 2024.

[7] IoT-Based Smart Energy Meter with Real-Time Monitoring and Theft Detection using Arduino and PZEM004T, Int. J. of Engineering Re- search and Technology, vol. 14, no. 12, 2025.

[8] M. Yedge et al., Smart Energy Meter and Theft Detection Using ESP32,

[9] IJRASET, 2025.

[10] K. H. Akhil et al., Enhanced Low-Cost Smart Energy Meter with Theft Detection using IoT, in Proc. IEEE 3rd Int. Conf. on Intelligent Manufacturing and Information Analytics (ICIMIA), 2023.

[11] B. K. Sahani and T. Ravi, IoT Smart Energy Meter System: A Review, Int. J. on Recent and Innovation Trends in Computing and Communi- cation, 2023.

[12] S. Karmakar et al., IoT Based Smart Electricity Energy Meter using ESP32 and Blynk Application, Journal of Sensor Research and Tech- nologies.

[13] IoT Smart Electricity Energy Meter, IJRASET, 2024.

[14] A. Sharma and R. Singh, IoT Based Smart Energy Meter for Real-Time Monitoring and Theft Detection, IJERT, 2021.

[15] S. K. Jain and V. P. Venkatesh, Electricity Theft Detection Techniques in Smart Grids, IEEE Trans. Power Systems, 2020.

[16] Q. Mahmoud et al., Deep Recurrent Electricity Theft Detection in AMI Networks, arXiv preprint arXiv:1809.01774, 2018.

[17] M. I. Ibrahem et al., Efficient Privacy-Preserving Electricity Theft Detection in AMI Networks, arXiv preprint arXiv:2005.13793, 2020.

[18] F. Kabir et al., RIOT-Based Smart Metering System for Privacy- Preserving Data Aggregation, arXiv preprint arXiv:2501.06161, 2025.

[19] Y. Kulkarni et al., EnsembleNTLDetect: An Intelligent Framework for Electricity Theft Detection, arXiv preprint arXiv:2110.04502, 2021.

[20] IoT Based Electricity Theft Detection System, STM Journals, 2025.

[21] M. Alenezi et al., An IoT Enabled Machine Learning Model for Energy Theft Prevention System in Smart Cities, Journal of Cloud Computing, 2023.

[22] Arduino, Arduino UNO Microcontroller Datasheet and Technical Doc- umentation, Arduino Official Documentation.

[23] Espressif Systems, ESP32 Technical Reference Manual, Espressif Sys- tems Inc.

[24] MathWorks, ThingSpeak IoT Analytics Platform Documentation.

[25] Blynk Inc., Blynk IoT Platform Documentation.

[26] IEEE Standards Association, IEEE Smart Grid Standards for Metering and AMI, IEEE Std. 1701 Series.