International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IoT-Driven Monitoring for Detecting and Preventing Electricity Theft in Power Networks

[1] Hemalatha P, [2] Poongodi P, [3] Indhu S, [4] Punitha A, [5] Santhiya S, [6] Saranya M,

[1,2]Assistant Professor, Department of Electrical and Electronics Engineering, Nandha College of Technology, Erode-638 052.
[3,4,5,6]UG-Final year, Department of Electrical and Electronics Engineering, Nandha College of Technology, Erode-638 052
[1] hema12latha@gmail.com,[2] ppoonga17@gmail.com ,[3] indhu.s2021@nandhatech.org ,[4] punithaanandan7@gmail.com,
[5] santhiya.dhanama93@gmail.com ,[6] saranya.muthaiyan2021@nandhatech.org

ABSTRACT

An IoT based monitoring system designed to detect and prevent electricity theft in power distribution networks. Electricity theft remains a major challenge, leading to significant revenue losses and affecting power quality and availability. The proposed system utilizes smart meters, CT (Current Transformer) and PT (Potential Transformer) sensors, and wireless communication modules to collect real-time data on energy consumption. This data is securely transmitted to a central server, where AI (Artificial Intelligence)-driven algorithms analyze usage patterns to identify anomalies such as unauthorized tapping or sudden drops in recorded consumption.

Upon detection of irregularities, the system generates real-time alerts to enable immediate action by utility personnel. The architecture is scalable, cost-effective, and suitable for deployment across both urban and rural regions. It leverages cloud-based storage and analytics for efficient data management and reporting. This IoT-driven solution not only reduces AT&C (Aggregate Technical and Commercial) losses but also improves transparency, operational efficiency, and system reliability. By enabling proactive monitoring and rapid response, the system supports fair electricity usage and helps build a smarter, more secure energy infrastructure. This innovative approach offers a sustainable and effective method for combating electricity theft in modern power networks.

KEYWORDS; IOT(Internet Of Things), PT (Potential Transformer), CT (Current Transformer), AI (Artificial Intelligence), AT&C (Aggregate Technical and Commercial).

1. INTRODUCTION

Electricity is a critical resource that fuels modern society's infrastructure, industry, and daily life. However, one of the most persistent challenges faced by power utilities worldwide is electricity theft.

It not only results in substantial economic losses but also affects the quality and reliability of the power supply. According to global estimates, billions of dollars are lost annually due to non-technical losses such as unauthorized connections, meter tampering, and bypassing of energy meters. These illegal practices not only put an undue burden on honest consumers but also degrade the overall efficiency and stability of power distribution networks.

Traditional methods of detecting electricity theft, such as manual inspections and audits, are time-consuming, labor-intensive, and often inefficient. With the increasing demand for energy and the growing complexity of electrical grids, there is an urgent need for smarter, automated, and more efficient solutions. This is where the Internet of Things (IoT) offers a promising approach. By embedding sensors, smart meters, and communication modules within the power network, IoT enables real-time monitoring, data collection, and analytics, allowing for proactive detection and prevention of electricity theft.

The integration of IoT technology in power networks allows for continuous observation of consumption patterns, voltage levels, and current flow. Any deviation from expected behavior—such as sudden drops in usage, abnormal load variations, or unexpected line losses—can be detected instantly. Smart meters equipped with CT (Current Transformer) and PT (Potential Transformer) sensors collect real-time data, which is transmitted to a centralized server using secure communication protocols. Here, advanced algorithms, often powered by Artificial Intelligence (AI), analyze the data to identify irregularities that may indicate theft.

The proposed IoT-based monitoring system not only helps detect theft but also improves overall grid transparency, enhances energy management, and reduces AT&C (Aggregate Technical and Commercial) losses. It allows for remote diagnostics, automatic alerts, and quick intervention, minimizing manual efforts and operational costs. Moreover, this system is scalable and adaptable, making it suitable for both urban and rural deployment.

Here, we explore the design, implementation, and benefits of an IoT-driven solution for electricity theft detection. We aim to demonstrate how real-time monitoring and intelligent data analysis can transform traditional power networks into smart, secure, and more efficient systems capable of withstanding the growing challenges in energy distribution.

2. PROPOSED SYSTEM

The proposed system is designed to detect and prevent electricity theft through real-time monitoring and intelligent control. It comprises a power conversion section, sensing modules, a central processing unit, display and communication interfaces, and control outputs. The architecture facilitates continuous tracking of electrical parameters such as voltage and current while enabling data-driven decision-making and remote alerts.

The system begins with a segment that converts high-voltage alternating current from the supply lines into a lower voltage level suitable for electronic circuitry. This conversion process includes rectification and smoothing to produce a consistent direct current output. The converted voltage is then stabilized and regulated into two different levels, each supporting different operational requirements within the circuit. These regulated voltages ensure the safety and reliability of all connected electronic components.

Following voltage regulation, the system includes a manual selector that allows switching between different voltage levels based on the connected load or testing needs. This switch provides flexibility, especially during system calibration or when deploying in various environmental conditions. The selected voltage passes through a sensing module designed to measure electrical potential. The measured values are then digitized for processing and analysis.

In parallel, the current flowing through the circuit is also continuously monitored using a dedicated sensing module. Any discrepancy in current flow, such as a sudden spike or drop, may indicate the presence of unauthorized consumption or tampering with the power lines. These signals, like voltage, are converted into a digital format and transmitted to the central control unit for further evaluation.

At the core of the system lies the control unit, a compact and efficient microcontroller capable of high-speed data processing and multi-channel communication. This controller receives input data from the voltage and current sensing units, analyzes the values, and applies programmed logic to determine whether the observed patterns are within acceptable ranges. If any anomaly is detected, it flags the condition and initiates a response mechanism.

To keep users or technicians informed, the system incorporates a visual display that shows key parameters such as current and voltage levels, system status, and fault indicators. This local interface ensures that system performance can be easily verified on-site without the need for additional equipment.

Beyond local monitoring, the system also features remote connectivity. A dedicated communication interface allows real-time data to be transmitted to cloud platforms or remote servers. Through this interface, anomalies can be reported immediately, allowing utility providers or administrators to receive alerts and respond swiftly, regardless of their physical location. This connectivity ensures comprehensive oversight and supports large-scale monitoring in urban and rural power grids.

In terms of actuation, the system can respond to detection events by controlling connected electrical loads. If unauthorized usage is suspected, the system can disconnect power to certain lines or devices, preventing further loss and ensuring safety. This response mechanism is coordinated by the central controller, which sends commands to the load interface module, enabling or disabling output devices as needed.

An additional feature of the system is its ability to simulate theft conditions through a dedicated output. This feature is crucial for testing and validating the theft detection capabilities of the system. By creating a scenario where unauthorized current is drawn, the system is tested on how quickly and accurately it can detect and respond to such events.

The design is modular and scalable, making it adaptable to a wide range of environments and use cases. Whether implemented in residential, commercial, or industrial settings, the system can be customized according to the scale of energy consumption and specific monitoring requirements. Its reliance on widely available components and open-source hardware also makes it economically feasible for large-scale deployment.

One of the key strengths of the system lies in its intelligent processing. By analyzing real-time data from multiple sensing points, it can differentiate between normal fluctuations and deliberate tampering. This ensures that alerts are not triggered by false positives, which would otherwise lead to unnecessary inspections and operational inefficiencies. The use of real-time digital processing allows for accurate decision-making, even in dynamic power environments.

Furthermore, the system is designed with robustness and reliability in mind. The protective power conversion section ensures that sensitive electronics are shielded from voltage surges or instability. The sensing modules are calibrated for precision, ensuring that even small irregularities are captured. The control unit is capable of multi-threaded operation, enabling it to process incoming data, update the display, communicate with remote servers, and manage loads simultaneously without delays.

Another valuable feature is its real-time visualization. By continuously updating the user interface, the system offers instant insights into its operating condition. This aids maintenance personnel in conducting quick diagnostics and ensures that performance bottlenecks or hardware failures are identified promptly.

From a communication standpoint, the system utilizes secure data protocols for uploading readings and event logs. This ensures data integrity and prevents tampering or unauthorized access. In power networks where safety and reliability are paramount, this level of security is critical.

Ultimately, the proposed system is a modern response to an age-old challenge. Electricity theft is not only a financial burden on utility providers but also a social issue that affects honest consumers and disrupts energy planning. By introducing a smart, connected, and autonomous monitoring solution, this system addresses the problem at its root—by detecting irregularities as they happen and responding swiftly to prevent loss.

Its real-world application is vast. It can serve as a standalone solution for single households or be integrated into smart grid infrastructures, supporting centralized monitoring across cities.

The modular nature ensures that it can evolve with technological advancements, such as artificial intelligence or machine learning, to further improve detection accuracy and predictive analytics.

Implementation of the proposed system:

- Built a power supply unit to convert AC to regulated 5V/12V DC.
- Connected voltage and current sensors to monitor real-time electrical data.
- Programmed ESP32 using Arduino IDE to read and analyze sensor values.
- Displayed voltage, current, and alerts on an LCD screen.
- Enabled Wi-Fi on ESP32 to send data to an IoT platform (like Blynk).
- Detected power theft when current flows without authorized load.
- Automatically disconnected load using a motor driver when theft occurred.
- Simulated theft by creating an illegal connection.
- Verified alert and control actions.
- Finalized setup after successful testing.

In the context this project is needed for several essential reasons:

1. Prevents Electricity Theft

Electricity theft causes huge losses to power providers. This system detects unauthorized usage in real-time and helps reduce theft effectively.

2. Ensures Fair Billing

By stopping illegal power use, honest consumers are protected from inflated bills caused by others' misuse.

3. Real-Time Monitorin

The IoT-based system allows live tracking of power usage, helping utility companies and users take quick action when theft is detected.

4. Saves Energy and Revenue

Minimizing power theft helps save energy and reduces financial losses for both governments and private electricity distributors.

5. Enhances Grid Security

It adds a smart layer of security to the power distribution network, making it more reliable and tamper-proof.

6. Supports Smart City Development

This aligns with modern smart grid and smart city goals, enabling intelligent and automated energy management.

3.SYSTEM ARCHITECTURE

The system architecture of this project is designed to effectively detect and prevent electricity theft using smart sensing, real-time processing, and IoT communication. The architecture consists of several integrated layers that work together to monitor electrical parameters, identify theft scenarios, and alert users or authorities through remote platforms. The architecture begins with the power conversion unit, which is responsible for supplying a stable DC voltage to all the electronic components in the system. This unit typically includes a step-down transformer, bridge rectifier, filter capacitors, and voltage regulators to convert the AC mains supply into regulated 5V and 12V DC outputs. These regulated voltages are essential for safely powering the microcontroller, sensors, display modules, and communication units.

The sensing layer, which comprises voltage and current sensors. The voltage sensor measures the line voltage, while the current sensor monitors the current drawn by the load. These sensors continuously collect data and convert it into analog signals. These analog signals are fed into the analog pins of the ESP32 microcontroller for further processing. The sensors play a vital role in detecting variations in load behavior and identifying unusual current flow that may indicate electricity theft. Proper calibration ensures accurate readings under various load conditions.

The core of the architecture is the processing layer, managed by the ESP32 microcontroller. This unit reads the input from the sensors using its built-in ADC (Analog-to-Digital Converter). The microcontroller is programmed to analyze the incoming voltage and current data in real-time.

It compares the current drawn by the load against the expected values. If it detects that current is flowing without proper authorization (e.g., bypassing the main load path), it identifies this condition as electricity theft. The microcontroller then triggers the necessary actions to respond to the situation.

The user interface layer consists of an LCD display that shows real-time system data such as voltage, current, and any warning or alert messages. This allows on-site users or technicians to instantly view the status of the system without needing to connect to a computer. It acts as the immediate feedback unit for the local environment.

The communication layer of the architecture is based on the IoT capability of the ESP32. Using its built-in Wi-Fi module, the ESP32 connects to a cloud platform like Blynk or Thingspeak. Through this platform, it uploads real-time sensor data and sends alerts when theft is detected. This feature allows users, utility companies, or monitoring teams to remotely access the system's data and receive instant notifications via smartphones or computers, improving responsiveness and system transparency.

The control and actuation layer ensures that if a theft condition is detected, the system responds by disconnecting the load using a motor driver circuit. This prevents further power misuse and enhances the security of the power distribution system. Altogether, the architecture is built to be cost-effective, scalable, and reliable for modern power systems.shown in fig.1.

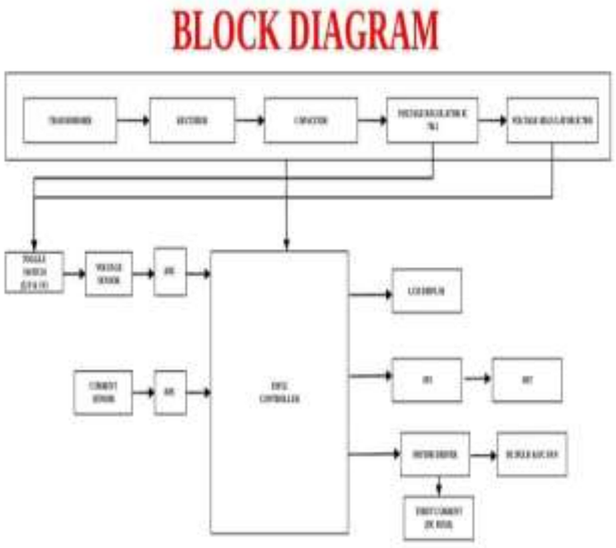


Fig.1.Block Diagram

3.1 ESP32 (Main Controller)

The ESP32 microcontroller reads real-time data from voltage and current sensors, processes it to detect abnormal usage or electricity theft, and displays the values on an LCD. It connects to Wi-Fi to send alerts to a cloud platform and automatically controls the load by turning it off during theft detection.shown in fig.3.1

Fig. 3.1

3.2 Transformer

The transformer steps down the 230V AC mains supply to a lower AC voltage, typically 12V. This reduced voltage is then converted to DC and regulated to power components like the ESP32, sensors, and display. It ensures safe, stable voltage for the system's proper operation.shown in fig.3.2

Fig. 3.2.

3.3 Serial Peripheral Interface

SPI enables fast communication between the ESP32 and SPI-compatible modules like an LCD. It transfers data using MOSI, MISO, SCK, and CS lines. The ESP32 acts as the master, sending sensor data to the display for real-time updates, ensuring accurate and quick monitoring in the system.shown in fig.3.3

Fig. 3.3

3.4 LCD Display

The LCD display shows real-time voltage, current, and system status based on sensor data processed by the ESP32. It receives commands and values through digital or SPI/I2C communication. This allows users to monitor power flow and theft alerts directly on the screen, ensuring quick local observation and feedback.shown in fig.3.4

Fig. 3.4

3.5 Voltage Regulator

The voltage regulator converts the unsteady DC voltage from the rectifier into a stable 5V or 12V output. It ensures that components like the ESP32, sensors, and display receive a consistent and safe voltage supply, preventing damage and maintaining reliable operation throughout the entire electricity theft detection system.shown in fig.3.5

Fig.3.5

3.6 Motor Driver Module

Measures voltage, current, power consumption (kWh), and energy usage patterns. sends real-time power consumption data to ESP32 for processing and helps in billing, monitoring energy efficiency, and detecting anomalies like power theft.shown in fig.3.6

Fig. 3.6

3.7 Current Sensor

The Power Control section in the Next-Gen Energy Meter with Load Control is responsible for monitoring, regulating, and displaying power parameters in real-time. It consists of three key components: current sensor and voltage sensor. These components work together to ensure accurate energy monitoring, overload protection, and efficient power control.shown in fig.3.7

Fig.3.7

3.8 Overall System Operation

1. Smart meters and sensors monitor voltage, current, and energy usage across different points in the power distribution network.

2. IoT devices transmit real-time data to a central system using secure protocols like LoRa, GSM, or Wi-Fi.

3. Centralized cloud servers analyze incoming data using AI algorithms to detect unusual patterns indicating possible electricity theft.

4. When anomalies are detected, the system generates immediate alerts for utility providers to take appropriate action.

5. Authorities respond by remotely disconnecting supply or dispatching teams to investigate and prevent further electricity theft.

4. HARDWARE IMPLEMENTATION

Electricity theft poses a serious threat to the efficiency and sustainability of power distribution systems. To counter this, the proposed project employs an IoT-based solution that combines several hardware components to monitor and detect unauthorized usage. The hardware setup starts with the installation of smart meters integrated with current and voltage sensors. These sensors are capable of capturing real-time data on electricity usage and any deviations from normal consumption patterns. The current sensor, such as ACS712 or a CT (current transformer) sensor, detects the amount of current flowing through the wire. Similarly, a voltage sensor monitors the voltage levels to detect abnormalities that may signal tampering or bypassing.

This sensor data is fed into a microcontroller, commonly an Arduino Uno or ESP32, which serves as the central processing unit for the system. The microcontroller collects and processes data continuously from the sensors. It converts analog signals into digital data for further processing.

The ESP32 is preferred in many cases due to its built-in Wi-Fi and Bluetooth capabilities, making it more efficient for IoT-based communication. Once the data is collected, it is analyzed to detect any discrepancies in power usage that may suggest theft.

To enable real-time monitoring, the microcontroller transmits the data wirelessly to a central server or cloud platform. This is made possible through communication modules like Wi-Fi (ESP8266/ESP32), GSM (SIM800L), or LoRa (Long Range Radio) modules. The choice of communication module depends on the geographical location and infrastructure available. In remote areas where internet connectivity is limited, LoRa or GSM modules are ideal due to their wide range and independence from Wi-Fi networks.

Power supply for the entire setup is crucial. A regulated power supply unit ensures stable voltage and current to the microcontroller and other components. In many installations, a 5V DC adapter or battery backup is used to maintain continuous operation even during power cuts, ensuring the integrity of data collection and transmission. A voltage regulator like the LM7805 may be employed to maintain consistent voltage to sensitive components.

Another important element of the hardware setup is the relay module. This component is integrated with the system to take action in case of detected theft. For instance, if abnormal activity is confirmed, the relay can be triggered to disconnect the electricity supply to the affected section. This not only helps in preventing further theft but also alerts the authorities in real time.

An LCD display is included in the system for local monitoring. This allows maintenance personnel or residents to view real-time data such as voltage, current, power consumed, and alert status. The display is typically a 16x2 or 20x4 LCD, interfaced with the microcontroller through an I2C module to reduce wiring complexity.

To house all these components, a compact and insulated enclosure is designed. This protects the electronics from environmental factors such as dust, heat, and moisture.

The enclosure also includes slots for wiring and adequate ventilation to prevent overheating. Safety considerations are prioritized by ensuring proper insulation and separation between high-voltage and low-voltage circuits.

The calibration of sensors is a vital step in the implementation. Before deployment, the current and voltage sensors are calibrated using reference loads and standard measuring instruments. This ensures the accuracy of the data collected and reduces the chances of false alerts or misreadings. The microcontroller code is also carefully developed and uploaded to handle sensor readings, data conversion, wireless communication, and system alerts effectively.

Testing and validation of the system are carried out in real-world conditions. The hardware is installed in a controlled environment where various theft scenarios, such as bypassing the meter or grounding the neutral wire, are simulated. The system’s response to these actions is observed to fine-tune the detection algorithm and improve sensitivity without triggering false positives.

In addition to theft detection, the hardware also supports preventive monitoring. Any attempt to tamper with the meter box, disconnect sensors, or interrupt power to the microcontroller is recorded and flagged. Some systems also include vibration or door sensors to detect physical tampering of the meter unit.

Integration with solar or renewable sources is also possible. In areas using hybrid power systems, the smart meter setup can be adapted to differentiate between grid power and renewable input. This ensures accurate billing and prevents manipulation through alternate supply lines.

5.CIRCUIT DIAGRAM

This circuit uses an ESP32 microcontroller with current sensors, voltage regulators, LCD display, and relay drivers to monitor electricity usage and detect theft via IoT communication and real-time alerts.

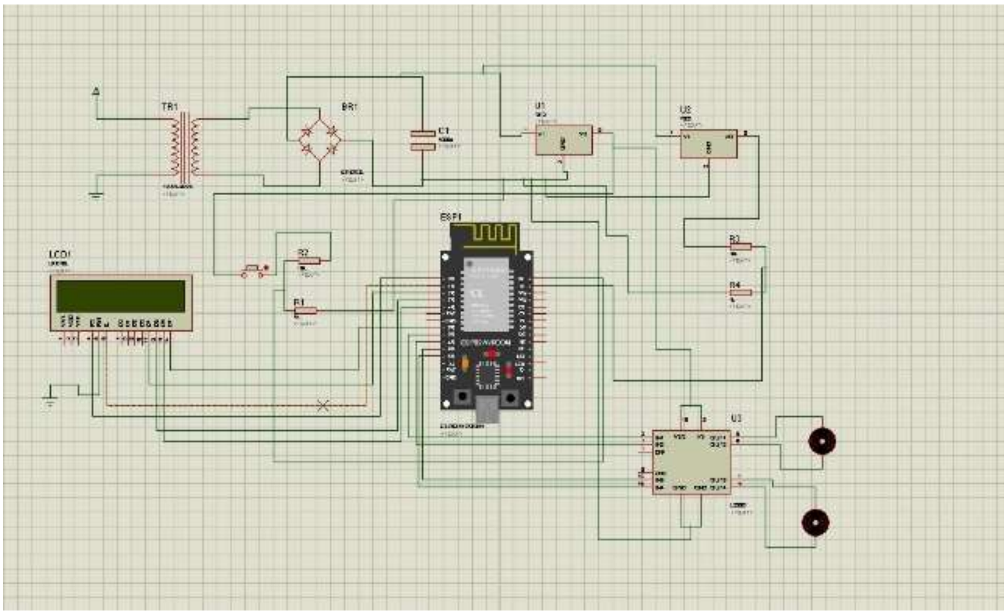


Fig.2.Circuit Diagram

The circuit appears to be an energy meter based on the ESP32 (ESP8266) microcontroller. It measures AC voltage and displays the power consumption on an LCD screen. Here's a breakdown of the components and their functions: [1]

- TR1 (Transformer): Steps down the AC voltage from the mains to a lower level suitable for the circuit.

- BR1 (Bridge Rectifier): Converts the AC voltage from the transformer to DC voltage.

- C1 (Capacitor): Filters the DC voltage to smooth out any ripples.

- U1 (Voltage Regulator): Regulates the DC voltage to a stable level for the ESP32 and other components.

- ESP1/ESP32 (Microcontroller): The brain of the circuit, it measures the voltage and current, calculates the power consumption, and controls the LCD display.

- R1 & R2 (Resistors): Form a voltage divider to scale down the voltage before it is measured by the ESP32.

- LCD1 (LCD Display): Displays the measured voltage, current, and power consumption.

- U3 (Motor Driver): Likely used to control a relay or other switching device, possibly for load control or calibration purposes.

- R3 & R4 (Resistors): Current-limiting resistors for LEDs or other indicators.

The circuit works by: [1, 2]

1.The AC voltage is stepped down by the transformer (TR1) and converted to DC by the bridge rectifier (BR1).

2. The DC voltage is filtered by the capacitor (C1) and regulated by the voltage regulator (U1).

3. The ESP32 measures the voltage and current using the voltage divider (R1 & R2) and an appropriate current sensing method (not clearly visible in the image).

4. The ESP32 calculates the power consumption and displays it on the LCD screen (LCD1).

5. The motor driver (U3) can be used to control external devices based on the measured power consumption.shown in fig.2.

6.SOFTWARE IMPLEMENTATION

The presented circuit diagram represents a smart IoT-based electricity theft detection and monitoring system. The heart of the design is the ESP32 microcontroller, which serves as the central control and communication unit. It is supported by a combination of sensors, voltage regulators, a display unit, relays, and a regulated power supply to form a complete working solution aimed at identifying and preventing electricity theft in power distribution networks.

The system begins with the power supply unit. The AC mains voltage is stepped down using a step-down transformer (TR1) to a lower AC voltage suitable for rectification. This AC voltage is then passed through a bridge rectifier (BR1) to convert it into DC. After rectification, a filter capacitor (C1) is used to smooth the voltage and reduce ripples. The filtered DC voltage is then regulated using two voltage regulators (U1 and U2)—typically 7805

ICs—which provide a steady 5V supply to the microcontroller and other components. This regulated voltage ensures that all electronic devices in the system operate reliably without being affected by power fluctuations.

Next in the system is the ESP32 microcontroller module, which performs the core processing and communication functions. It reads data from the sensors, processes the information, displays relevant details on the LCD screen, and sends it wirelessly to a remote server or monitoring system. The ESP32 is chosen due to its built-in Wi-Fi and Bluetooth capabilities, making it an ideal choice for IoT applications. It has multiple GPIO (General Purpose Input/Output) pins used for interfacing with the other components.

To monitor the electricity usage, the circuit includes current sensors connected near the load terminals. These sensors—most likely current transformers (CTs)—are connected to an op-amp-based signal conditioning circuit (U3) that amplifies and filters the analog signal from the CTs.

The output of this conditioning circuit is then fed to the analog pins of the ESP32. The microcontroller samples the analog current values and calculates the energy consumption based on pre-programmed logic. This value can be compared with the expected consumption, and any abnormal or sudden changes can trigger an alert for possible theft.

An LCD display (LCD1) is connected to the ESP32 to show real-time data, including voltage, current, and alert status. This LCD, likely a 16x2 type, is interfaced using standard data pins, and an I2C module may be used to reduce pin usage. The display is important for local monitoring, especially during maintenance or inspections.

The system also includes two relay modules, which are driven by the ESP32 through GPIO pins. These relays are used to control the power supply to the load. In case electricity theft is detected—such as tapping power before the meter or bypassing the current sensor—the ESP32 can activate the relays to disconnect the power supply temporarily or permanently, depending on the logic programmed. This feature adds a layer of automatic control and immediate action in response to unauthorized consumption.

Switches (R2 and others) shown in the diagram are used for manual control or resetting the system. These can serve as test switches to simulate fault conditions or theft scenarios during development and testing. Pull-down resistors (R1, R3, R4) are connected to ensure the microcontroller's input pins read stable values when the switches are not pressed.

Another key aspect of the circuit is the communication capability. Since ESP32 includes Wi-Fi, it can send real-time data to a cloud server or a local server depending on network availability. The data can include power consumption logs, detected anomalies, and action logs (like relay disconnection events).

This information can be accessed by utility companies or users through a web interface or a mobile app. In advanced versions, this system could include MQTT or HTTP protocols for secure and efficient communication.

The physical implementation of this circuit would involve careful layout and component placement. The current transformers must be placed accurately around live or neutral wires depending on the configuration. Adequate isolation should be maintained between the high-voltage section (transformer and AC lines) and low-voltage components (ESP32, LCD, etc.). For safety, opto-isolators may be used between relays and the microcontroller, though not shown in the schematic. Components should be housed in a proper insulated enclosure to protect against environmental hazards and accidental contact.

To ensure reliable and accurate operation, calibration is required. The CT sensors and voltage inputs must be calibrated using known loads and voltage sources. The software inside the ESP32 is responsible for converting sensor readings into meaningful data like watts, kilowatt-hours, and identifying thresholds beyond which alerts should be raised. This firmware can be developed using the Arduino IDE or the ESP-IDF framework, allowing flexibility in implementation.

Additionally, the system can incorporate anti-tamper mechanisms. Physical tampering of the box, disconnection of sensors, or attempts to reset the ESP32 without authorization can be detected using vibration sensors, magnetic contact sensors, or digital security checks coded into the firmware. Upon detection of tampering, the system can log the event and send an alert to the server immediately.

To further enhance the system, backup power using a small Li-ion battery or a supercapacitor can be added to keep the ESP32 running for some time during power outages. This allows for data transmission even during blackouts, which is useful for detecting sudden power cuts that could relate to theft attempts.

In real-world implementation, multiple such circuits can be deployed across different transformers, feeder lines, or customer locations. All these units can report to a central monitoring dashboard, enabling utility providers to analyze energy patterns, detect large-scale anomalies, and make informed decisions. Data analytics and machine learning algorithms can be layered on top to make the detection more intelligent over time.

In conclusion, the circuit diagram demonstrates a well-structured IoT solution to the problem of electricity theft. It combines real-time sensing, processing, display, communication, and control in a compact form. With careful calibration, programming, and deployment, such a system can significantly reduce power losses due to theft and improve the overall efficiency and security of the power distribution network. This hardware-driven solution, when paired with software intelligence, can bring about transformative changes in how energy is monitored and managed in smart grids.

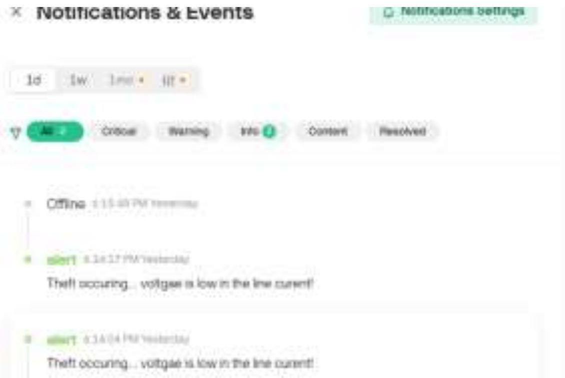
7.RESULT

The result of the project clearly demonstrates the effective functionality of the IoT-based electricity theft detection system. As shown in the notification log, the system successfully identified abnormal conditions in the power line, specifically indicating a drop in voltage and current a strong indication of possible electricity theft or tampering. The ESP32 microcontroller continuously monitored sensor inputs and triggered alerts when suspicious activities were detected. These alerts were transmitted in real-time to a cloud-based dashboard, where they were displayed with timestamps and categorized under critical information.

Overall, the project outcome proves that this IoT driven approach is not only functional but also scalable.

The system also logged offline activity, suggesting a possible power cut or intentional disconnection, which can be associated with theft attempts. These results validate the system's capability to track and report power anomalies, providing actionable data to utility providers. Additionally, the real-time alert mechanism allows for quick intervention and helps in minimizing power losses.

It enhances transparency and security in power distribution systems and can be implemented widely for smart grid management. With further refinement, it can serve as a valuable tool in the fight against electricity theft in both urban and rural areas**.**shown in fig.3.



Offline 4:15:40 PM Yesterday

alert 4:14:17 PM Yesterday
Theft occuring... voltgae is low in the line current!

alert 4:14:04 PM Yesterday
Theft occuring... voltgae is low in the line current!

Fig.3.Web Result

REFERENCES

[1] A. Kumar, R. S.S.S. R.D. S.R.R. and P. V. K. P. R. N., "IoT-based intelligent monitoring system for electricity the ft detection ,"IEEE Access,vol.11,pp.25334-25347,2023.

[2] A.M.S.F.I.K. and P.S.N.," Machine Learning based electricity theft detection system insmart grids," IEEE Transactions on Industrial Informatics, vol. 21, no. 7, pp. 1321-1328, July 2024.

[3] S. J. S. A. P. and M. T. H., "Electricity theft detection using IoT and data analytics," IEEE Internet of Things Journal, vol. 15, no. 6, pp. 5245-5256, June 2024.

[4] R.T.M.A.andP.V.B.,"Real-timeelectricity theft detection using IoT and machine learning algorithms," IEEE Transactions on Power Delivery, vol. 39, no. 8, pp. 4291-4299, 2024.

[5] G. P. H. K. and S. R. M., "A hybrid IoT and machinelearning based framework for electricity theft detection," IEEE Sensors Journal, vol. 23, no. 2, pp.950-959,February 2024.

[6] R.L.K. and A.S.K., "Anomaly detection for electricity theft prevention in smart grids using IoT," IEEE Transactions on Smart Grid, vol. 15, no. 9, pp. 4132-4140, September 2023.

[7] L.K.S. and R.T.M., "IoT -based solutions for smart grid theft detection: A survey," IEEE Transactions on Sustainable Energy, vol. 12, no.5, pp. 3412-3420, May 2024.

[8] H.A.M.A. and J.K.T., "Smart grid technology for reducing electricity theft :An IoT perspective," IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 25632570, April 2023.

[9] V.B.S. and A.L.N., "Data-driven electricity theft detection using machine learning in IoT networks," IEEE Transactions on Computational Intelligence, vol. 20, no. 3, pp. 456-465, March 2024.

[10] P.A.J and M.C.F" Real-time the ft detection and prevention in smart grids using IoT sensors, "IEEE Journal on Selected Areas in Communications, vol.42, no. 2, pp. 487-495, February 2024.

[11] J. C. F. and D. G. H., "A deep learning approach to electricity theft detection in IoT-based systems," IEEE Transactions on Neural Networks and Learning Systems, vol.35, no.5, pp.1051-1060, May 2024.

[12] R. P. S. and S. K. P., "IoT-based monitoring system for electricity theft detection in smart grids," IEEE Systems Journal, vol.13, no.3, pp.1115-1123, July2023.

[13] T. L. M. S. and J. P. D., "IoT-driven solution for real-time electricity theft detection," IEEE Transactions on Industrial Electronics, vol.68, no.1, pp.234-245, January 2024.

[14] G. B. Mohankumar, Dr. S. Manoharan,“ Performance Analysis Of Multi Converter Unified Power Quality Conditioner Using PI controller” Australian Journal of Basic and Applied Science7(9),331-340, 2013.

[15] J. Kumaresan, C. Govindaraju “PV tied three-port DC–DC converter operated four-wheel-drive hybrid electric vehicle” Electrical Engineering102(4),2295-2313, 2020.