International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 01 | Jan 2026 www.irjet.net p-ISSN: 2395-0072

An Intelligent Power Theft Detection and Load Profiling System

Katragadda Harini [1], Tirumalasetty Jahnavi[2], Gudeti Sudarshan Aravind Reddy[3] , Rudrapankthi Naveen [4], Reddiboina Leela Krishna[5] , Nanduri Tejaswini[6]

[1,2,3,4,5,6]*BTech in ECE & VVIT,Andhra Pradesh,India`*

Abstract - *Electricity theft remains one of the most critical challenges faced by modern power distribution systems, particularly in developing regions where monitoring infrastructure is limited. Practices such as illegal tapping, meter bypassing, and physical tampering of energy meters result in significant revenue losses for utility providers and adversely affect grid stability and power quality. Conventional electricity meters are primarily designed for billing purposes and do not possess real-time monitoring, analytical intelligence, or communication capabilities required for effective theft detection.*

This paper presents an ESP32-based intelligent power theft detection and load profiling system that continuously monitors voltage and current parameters to compute real-time power and energy consumption. The proposed system introduces load profiling through statistical analysis of historical consumption data, enabling the identification of abnormal usage patterns. In addition, tamper detection mechanisms are implemented to monitor electrical irregularities and physical disturbances in the metering system. Time-of-use analysis is incorporated to detect suspicious energy consumption during predefined off-peak or low-activity periods, which is a common indicator of unauthorized usage. Illegal tapping scenarios are experimentally simulated by introducing unregistered loads to evaluate the effectiveness of the detection methodology.

The ESP32 microcontroller performs local data processing and anomaly detection while transmitting energy data and alerts to a cloud-based dashboard using integrated Wi-Fi communication. Experimental results demonstrate that the system can detect abnormal load variations, illegal tapping, and tampering events with low latency and acceptable accuracy. The proposed solution is cost-effective, scalable, and suitable for residential and small commercial applications, contributing to enhanced transparency, improved theft detection, and smarter energy management within modern power distribution networks.

Key Words: **Power Theft Detection, Load Profiling, ESP32, Smart Energy Meter, Tamper Detection, Time-of-Use Analysis, IoT, Energy Monitoring**

1.INTRODUCTION

Electric power distribution systems form the backbone of modern society, supporting residential, commercial, and industrial activities. With rapid urbanization and increasing dependence on electrical energy, the demand placed on power grids has grown significantly. Alongside this growth, electricity theft has emerged as a major concern for utility providers worldwide. Electricity theft not only causes substantial financial losses but also leads to increased transmission losses, voltage fluctuations, transformer overloading, and degradation of overall grid reliability.

Electricity theft can take various forms, including illegal tapping of distribution lines, bypassing of energy meters, manipulation of metering circuitry, and unauthorized extension of loads. These activities often occur intermittently and are difficult to detect using conventional monitoring approaches. In many regions, theft detection relies on manual inspection and post-billing analysis, which are inefficient, time-consuming, and prone to human error. As a result, theft activities may continue undetected for extended periods.

Traditional metering infrastructure lacks the capability to analyse consumption patterns or identify abnormal behaviour in real time. The absence of communication and intelligence at the meter level further limits the ability of utilities to respond quickly to suspicious activities. With the emergence of smart grid concepts, there is a growing need for intelligent, distributed monitoring systems that can operate at the consumer end and provide actionable insights to utility providers.

Recent advancements in embedded systems and Internet of Things (IoT) technologies have enabled the development of smart energy meters capable of real-time data acquisition, processing, and communication. Embedded controllers with integrated wireless connectivity allow continuous monitoring of electrical parameters and remote visualization of energy usage. Load profiling, tamper detection, and time-of-use analysis are increasingly being recognized as effective techniques for identifying abnormal consumption behaviour and potential theft events.

1.1 Traditional Energy Metering System

Traditional energy metering systems are designed primarily to measure cumulative electrical energy consumption over a specified billing period. These systems are typically electromechanical or basic electronic meters that integrate voltage and current over time to calculate energy usage in kilowatt-hours. Meter readings are collected periodically, either manually by utility personnel or through basic automated meter reading mechanisms.

While conventional meters are reliable for basic energy measurement and billing, they lack intelligence and real-time monitoring capabilities. They do not provide information about instantaneous power consumption, load variations, or time-based usage patterns.. As a result, utilities are unable to distinguish between normal and abnormal consumption behavior using traditional meters alone.

Electricity theft detection in traditional systems relies heavily on manual inspection of distribution lines and meters. Utility personnel may compare billed energy with transformer output or inspect physical connections to identify illegal tapping. These methods are reactive in nature and depend on human judgment, making them inefficient and inconsistent. Short-duration or intermittent theft activities are particularly difficult to detect using such approaches.

Furthermore, traditional meters do not support communication with centralized monitoring systems. The absence of real-time data transmission prevents utilities from responding promptly to suspicious activities. In the context of increasing electricity demand and complex distribution networks, the limitations of traditional energy metering systems highlight the need for intelligent alternatives capable of real-time analysis and decision-making.

1.2 Limitations of Existing Methods

Existing electricity theft detection methods suffer from several limitations that restrict their effectiveness in practical scenarios. Manual inspection-based approaches are labour-intensive, time-consuming, and costly. They require frequent field visits and are susceptible to human error, making them unsuitable for large-scale deployment. Post-billing analysis techniques compare historical consumption data to identify discrepancies. However, such methods are inherently delayed and fail to detect theft in real time. They are also ineffective in identifying short-term or intermittent theft activities that do not significantly affect monthly billing totals.

Some advanced systems rely on centralized data analytics or complex machine learning models to detect theft patterns. While these approaches can offer improved accuracy, they often require high computational resources and extensive datasets. This increases system complexity and cost, making them unsuitable for low-cost embedded implementations at the consumer end.

Additionally, many existing solutions focus solely on energy consumption discrepancies and ignore other important indicators such as physical tampering, time-of-use behaviour, and sudden load variations. The lack of integrated tamper detection and time-based analysis reduces the reliability of theft identification and increases false positives.

These limitations emphasize the need for a decentralized, intelligent system capable of local data processing, real-time anomaly detection, and remote reporting, while remaining cost-effective and scalable.

1.3 Proposed System

The proposed system utilizes an ESP32 microcontroller as the core processing unit due to its high processing capability, low power consumption, and integrated Wi-Fi connectivity. Voltage and current sensors are interfaced with the ESP32 to continuously measure electrical parameters. Using these measurements, the system calculates instantaneous power and cumulative energy consumption in real time.

Load profiling is performed by analysing historical consumption data collected over extended periods. Statistical parameters such as average load, peak demand, and time-based usage trends are used to establish normal consumption profiles. Deviations from these profiles, including sudden load spikes and unusual consumption patterns, are identified as potential theft indicators.

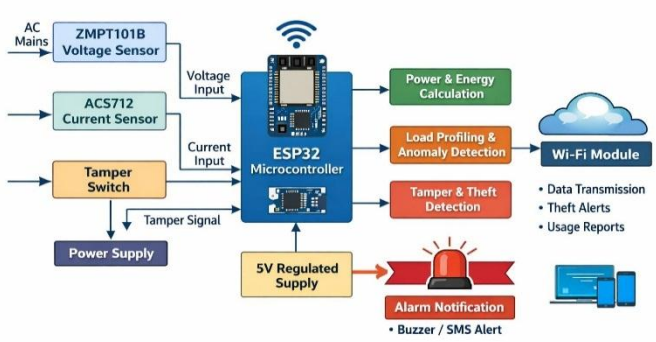

***Fig -1**: Block Diagram*

Tamper detection mechanisms are incorporated to monitor abnormal electrical behaviour and physical disturbances. These include sudden loss of sensor signals, unexpected voltage variations, and abrupt changes in current flow that may indicate meter bypassing or manipulation. Time-of-use analysis further enhances detection by identifying energy usage during predefined off-peak or restricted periods, which is a common characteristic of unauthorized consumption.

Illegal tapping scenarios are experimentally simulated by connecting unauthorized loads parallel to the monitored line. This allows evaluation of the system's ability to detect unregistered consumption through abnormal current signatures and load variations. Upon detecting suspicious activity, the ESP32 transmits alerts and energy data to a cloud-based dashboard using Wi-Fi communication.

The proposed system combines real-time sensing, local intelligence, and IoT-based monitoring into a single platform. It offers a scalable and economical solution for improving theft detection, enhancing energy transparency, and supporting the development of smarter power distribution networks.

Table -1: Detection Scenarios and System Response

Scenario	Detection Method	System Response
Normal Load	Profile Matching	No Alert
Sudden Load Spike	Threshold Deviation	Theft Alert
Off-Peak Usage	Time-of-use Analysis	Suspicious Activity
Meter Box Opened	Reed Switch	Tamper Alert
Illegal Tapping	Current Anomaly	Theft Alert

2. Hardware Requirements

The proposed intelligent power theft detection and load profiling system is developed using low-cost, reliable, and commercially available hardware components. The hardware architecture is designed to support continuous monitoring of electrical parameters, real-time processing, tamper detection, and wireless data transmission. The system is intended to function as a smart energy monitoring unit deployed at the consumer end.

Each hardware component is selected to ensure measurement accuracy, operational reliability, and ease of integration with the embedded controller. The overall design emphasizes scalability and robustness while maintaining simplicity and cost effectiveness.

2.1 ESP32 Microcontroller Unit

The core processing unit of the system is the ESP32 Dev Module (ESP32-WROOM-32). This module is selected due to its integrated Wi-Fi capability, high processing speed, and suitability for real-time embedded applications. The ESP32 operates at a clock frequency of up to 240 MHz and includes sufficient SRAM and flash memory for data processing, logging, and communication tasks.

The ESP32 is responsible for:

- Interfacing with voltage and current sensors
- Sampling analog signals using the internal ADC
- Computing real-time power and energy values
- Executing load profiling and anomaly detection algorithms
- Managing tamper detection inputs
- Transmitting data and alerts to the cloud dashboard via Wi-Fi
  Local processing on the ESP32 minimizes

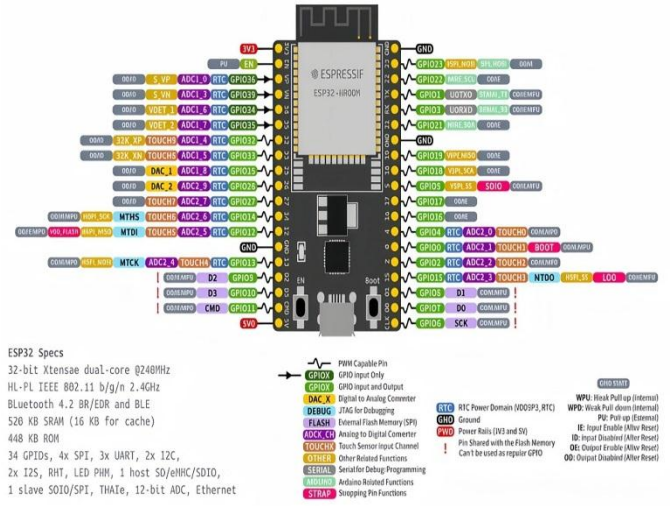

Fig -2: *ESP32 Microcontroller*

Detection latency and enables real-time decision-making at the meter level.

2.2 Voltage Sensor Module

Voltage measurement is implemented using the ZMPT101B AC voltage sensor module. This sensor provides electrical isolation between the high-voltage mains and the low-voltage embedded circuitry, ensuring safe operation. The module outputs an analog signal proportional to the input AC voltage.

The ESP32 continuously samples the voltage sensor output and converts the raw analog values into digital form using its ADC. Software-based calibration is applied to map ADC readings to actual voltage values. This calibration improves measurement accuracy and compensates for sensor tolerances.

Real-time voltage monitoring enables the detection of abnormal voltage conditions such as sudden drops or fluctuations. These conditions may indicate meter bypassing, supply irregularities, or tampering, and are therefore treated as important indicators during anomaly detection.

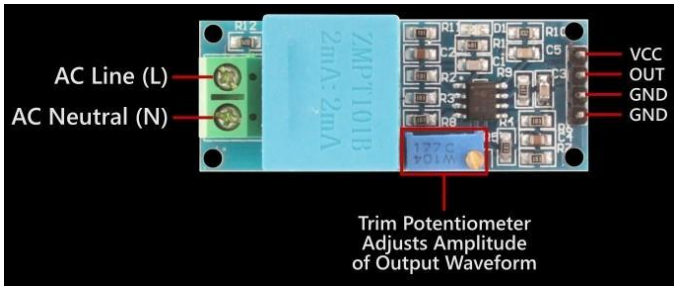

Fig -3: *Voltage Sensor Module*

2.3 Current Sensor Module

Current measurement is carried out using the ACS712-20A Hall-effect current sensor module. The sensor provides galvanic isolation and outputs a linear analog voltage proportional to the load current flowing through the circuit. It is well suited for residential and small commercial current ranges.

The analog output of the current sensor is sampled by the ESP32 at fixed intervals. Offset calibration and noise reduction techniques are applied in software to eliminate zero-drift and improve measurement stability. Accurate current measurement is essential for reliable power calculation and load profiling.

Sudden increases in current or unexpected variations in current patterns are closely monitored. Such deviations often indicate illegal tapping or unauthorized load connections, making current sensing a critical component of theft detection.

Fig -4*: Hall-effect Current Sensor*

2.4 Tamper Detection Hardware

Tamper detection is implemented using both physical and electrical monitoring mechanisms to improve reliability. A reed switch or limit switch is installed inside the meter enclosure to detect unauthorized opening of the meter box. When the enclosure is opened, the switch state changes and is detected by the ESP32 through a digital input pin. In addition to physical monitoring, electrical tamper detection is implemented by observing inconsistencies in voltage and current sensor signals. Sudden loss of sensor output, abnormal signal behavior, or unexpected disconnection of sensing modules are treated as tamper events. This dual-layer tamper detection approach ensures that both physical manipulation and electrical bypassing attempts are identified promptly, reducing the likelihood of undetected theft.

2.5 Illegal Tapping Simulation Setup

Illegal tapping is experimentally simulated by connecting an unauthorized resistive load in parallel with the monitored circuit. This load bypasses the sensing path and introduces additional current consumption that does not match the established load profile. The simulated tapping setup allows controlled testing of the system's detection capability under realistic theft scenarios. Sudden current increases and abnormal consumption patterns generated by the unauthorized load are used to evaluate detection accuracy and response time.

This experimental approach enables validation of the proposed methodology without requiring complex external infrastructure or large-scale deployment.

2.6 Power Supply Unit

The system is powered using a regulated 5 V power supply derived from a step-down transformer or switched-mode power supply adapter. An LM2596 DC-DC buck converter module is used to provide stable voltage levels required by the ESP32 and sensor modules. Proper voltage regulation ensures reliable operation and prevents malfunction due to voltage fluctuations. Additional protection components such as capacitors and fuses are included to improve system durability and electrical safety.

3. Software Requirements

The software architecture of the proposed system is designed to support real-time data acquisition, intelligent analysis, anomaly detection, and IoT-based communication. The embedded firmware running on the ESP32 coordinates all system functions while maintaining reliable and deterministic operation.

A modular programming approach is adopted to improve readability, maintainability, and future extensibility of the software.

3.1 Development Environment and Programming Language

The embedded firmware is developed using the Arduino IDE and programmed in Embedded C/C++. The ESP32 Arduino core is used to access hardware peripherals and communication interfaces. This development environment provides extensive library support and simplifies firmware development and debugging.

Structured programming practices are followed to ensure clarity and reliability. Separate software modules are implemented for sensor interfacing, power calculation, anomaly detection, and communication.

3.2 Sensor Data Acquisition and Processing

Voltage and current sensors are sampled at fixed intervals using the ESP32's 12-bit analogy-to-digital converter. Multiple samples are averaged to reduce noise and improve measurement accuracy. Offset calibration is applied to compensate for sensor drift and environmental variations.

Filtered sensor data is used to compute RMS voltage and current values. These processed values form the basis for power calculation and subsequent analysis.

3.3 Power and Energy Calculation

Instantaneous power is calculated using real-time voltage and current values. Energy consumption is computed by integrating power over time using discrete sampling intervals. These calculations are performed locally on the ESP32, enabling real-time monitoring and reducing dependence on cloud-based processing.

3.4 Load Profiling Technique

Load profiling is implemented using a statistical threshold-based approach. Historical consumption data is recorded over time to establish normal usage patterns for a given consumer. Parameters such as average load, peak demand, and hourly energy consumption are calculated and stored. Real-time measurements are continuously compared with these reference values to identify abnormal behaviour.

3.5 Time-of-Use Analysis

Time-of-use analysis divides the day into predefined intervals such as peak hours, off-peak hours, and low-activity periods. Separate consumption profiles are maintained for each interval. Energy usage during off-peak or restricted periods is closely monitored. Unexpected consumption during these intervals is flagged as suspicious and contributes to theft detection decisions.

3.6 Tamper Detection Logic

Tamper detection logic continuously monitors the status of enclosure switches and sensor signals. A change in switch state or abnormal sensor behaviour triggers a tamper alert. Detected tamper events are logged locally and transmitted to the cloud dashboard for immediate notification and further investigation.

3.7 Illegal Tapping Detection Technique

Illegal tapping is detected using current anomaly detection techniques. Sudden current increases that exceed learned statistical thresholds without corresponding changes in normal load behaviour are classified as unauthorized connections. This lightweight detection technique is well suited for low-cost embedded systems and avoids the complexity of advanced machine learning models.

3.8 Cloud Communication and Data Logging

The ESP32 transmits real-time data and alerts to a cloud-based dashboard using Wi-Fi communication and HTTP protocol. The dashboard provides visualization of voltage, current, power, and energy trends. Historical data storage supports performance evaluation, event analysis, and future system improvements.

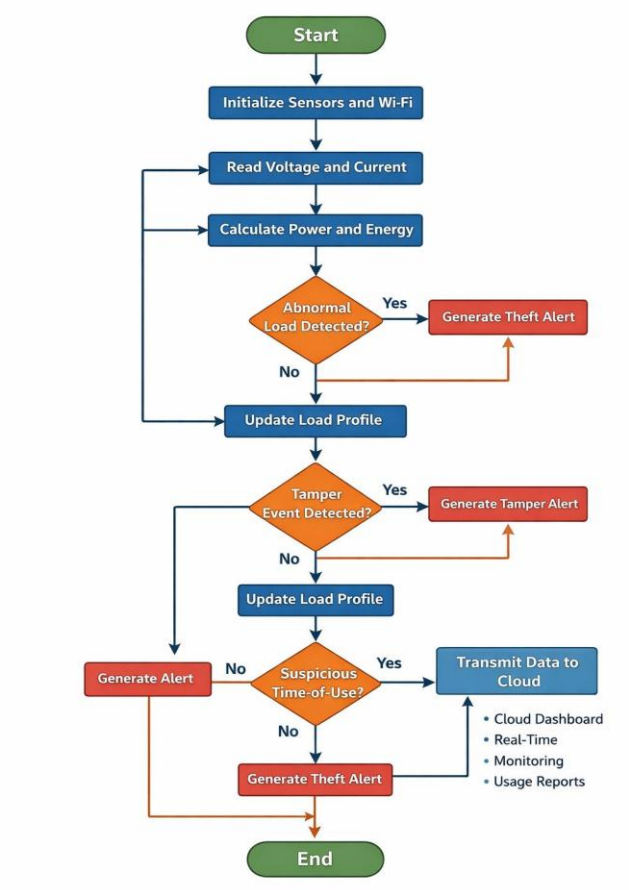

***Fig -5**: Flowchart*

4. Mathematical Modelling and Equations

Accurate computation of electrical parameters is fundamental to the proposed intelligent power theft detection system. The ESP32 performs real-time calculations using sampled voltage and current values obtained from the sensing modules.

The instantaneous power consumed by the load is calculated using the standard electrical relationship:

$P(t) = V(t) \times I(t)$

Where V(t) represents the instantaneous voltage and I(t) represents the instantaneous current at time t.

The RMS values of voltage and current are calculated from sampled data using:

$V_{rms} = \text{sqrt}((1/N) \times \Sigma(V_n^2)),\quad n = 1 \text{ to } N$

$I_{rms} = \text{sqrt}((\Delta t\ 1/N) \times \Sigma(I_n^2)),\quad n = 1 \text{ to } N$

Energy consumption is computed by integrating power over time using discrete sampling intervals:

$E = \Sigma(P_k \times)$, $k = 1$ to M
Where Δt is the sampling interval and P_k is the instantaneous power at the k^{th} sample.

These equations are implemented directly in the embedded firmware and executed locally on the ESP32 to enable real-time monitoring and analysis.

5. Algorithm and Pseudo-code

- **Algorithm 1: Load Profiling and Anomaly Detection**

The proposed system uses a statistical threshold-based algorithm to detect abnormal energy consumption patterns. The algorithm continuously compares real-time measurements with learned load profiles.

Pseudo-code:

```
Initialize system parameters
Initialize voltage and current sensors
Initialize Wi-Fi communication

While system is running:
  Read voltage sensor
  Read current sensor
  Calculate RMS voltage and RMS current
  Calculate instantaneous power
  Update cumulative energy

  Update load profile statistics
  Calculate deviation from average load
  If deviation > threshold:
    Flag abnormal load event
  If consumption during off-peak hours:
    Flag time-of-use anomaly
  If sensor signals missing or enclosure opened:
    Flag tamper event
  Transmit data and alerts to cloud dashboard
End While
```

This lightweight algorithm avoids complex computation while providing reliable detection suitable for embedded systems.

- **Algorithm 2: Illegal Tapping Detection**

Illegal tapping is identified by detecting sudden current increases without corresponding voltage changes.

Pseudo-code:

```
Monitor current continuously
Store previous current value

If (current – previous current) > tapping threshold:
  If voltage remains within normal range:
    Declare illegal tapping event
    Generate alert
End If

Update previous current
```

This approach effectively detects unauthorized load connections and minimizes false positives.

6. CONCLUSIONS

This paper presented the design and implementation of an intelligent power theft detection and load profiling system based on the ESP32 microcontroller. The proposed system addresses the limitations of conventional electricity meters by enabling real-time monitoring, local data processing, and remote reporting of electrical parameters. By continuously measuring voltage and current, the system accurately computes power and energy consumption while maintaining low cost and ease of deployment.

The integration of statistical load profiling allows the system to learn normal consumption behaviour over time and distinguish it from abnormal usage patterns. Sudden load variations, unexpected current spikes, and irregular consumption trends are effectively identified using threshold-based analysis. This approach avoids the complexity of computationally intensive machine learning models while remaining well suited for embedded platforms with limited resources.

Tamper detection mechanisms further enhance system reliability by monitoring both physical and electrical disturbances. Unauthorized opening of the meter enclosure and abnormal sensor behaviour are promptly detected and reported. The inclusion of time-of-use analysis strengthens theft detection by identifying suspicious energy consumption during off-peak or low-activity periods, which is a common characteristic of illegal electricity usage.

Illegal tapping scenarios were experimentally simulated by introducing unauthorized loads parallel to the monitored circuit. The results demonstrate that the proposed system can successfully detect such events through abnormal current signatures and deviations from established load profiles. The ESP32's integrated Wi-Fi capability enables real-time transmission of energy data and alerts to a cloud-based dashboard, allowing remote monitoring and faster response to theft incidents.

Overall, the proposed system provides a practical, scalable, and cost-effective solution for enhancing electricity theft detection and energy transparency in residential and small commercial applications. By combining real-time sensing, embedded intelligence, and IoT-based communication, the system contributes toward the development of smarter and more secure power distribution networks.

Future work may focus on extending the system to three-phase power systems, integrating advanced data analytics or machine learning techniques for improved detection accuracy, and implementing secure communication protocols for enhanced data protection. The proposed architecture serves as a strong foundation for next-generation smart metering and intelligent energy management systems.

REFERENCES

[1] D. P. Divan and H. Johal, "Distributed FACTS—A new concept for realizing grid power flow control," IEEE Transactions on Power Electronics, vol. 22, no. 6, pp. 2253–2260, Nov. 2007.

[2] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," Critical Information Infrastructures Security, Springer, pp. 176–187, 2009.

[3] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, "Nontechnical loss detection for metered customers in power utility using support vector machines," IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162–1171, Apr. 2010.

[4] A. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[5] M. F. Shaaban, A. Mohamed, and K. M. Nor, "A load profiling-based electricity theft detection system," International Journal of Electrical Power & Energy Systems, vol. 78, pp. 461–472, Jun. 2016.

[6] 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.

[7] H. Patel and R. Sharma, "Design and implementation of IoT based smart energy meter," International Journal of Engineering Research & Technology, vol. 9, no. 4, pp. 112–118, 2020.

[8] M. R. Alam, M. St-Hilaire, and T. Kunz, "An overview of m. Patel and R. Sharma, "Design and Development of an Autonomous Agricultural Robot for Sowing and Irrigation," Proceedings of the International Conference on Robotics and Automation in Agriculture, pp. 45–52, 2021.achine learning based methods for electricity theft detection," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2574–2593, 2019.

[9] A. Jain and S. Patel, "IoT based smart energy meter for efficient energy management," International Journal of Advanced Research in Computer Engineering & Technology, vol. 8, no. 6, pp. 145–151, 2019.

[10] EspressifSystems,"ESP32SerieDatasheet,"EspressifSystemsInc.,2023.[Online].Available: https://www.espressif.com

[11] Arduino, "Arduino IDE Documentation," [Online]. Available:https://www.arduino.cc/en/software

[12]AllegroMicrosystems,"ACS712Hall-EffectCurrentSensorDatasheet,"[Online].Available: https://www.allegromicro.com

[13]ZemingElectronics,"ZMPT101BACVoltageSensorModuleDatasheet,"[Online].Available: https://www.zeming.com.cn

[14] R. K. Singh and V. Verma, Embedded Systems and IoT in Smart Grid Applications, Wiley, 2021.

[15] M. Erol-Kantarci and H. T. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid," IEEE Communications Magazine, vol. 50, no. 5, pp. 34–40, May 2012.

[16]S. Mishra and P. Kumar, IoT Based Smart Metering and Energy Management, Springer, 2020.

[17] P. G. Da Silva, D. Ilić, and S. Karnouskos, "The impact of smart grid prosumer grouping on forecasting accuracy," IEEE Transactions on Industrial Electronics, vol. 62, no. 7, pp. 4319–4328, Jul. 2015.

[18] G. G. Dranka and A. Ferreira, "Power quality monitoring and analysis in smart grids," IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3512–3520, Jul. 2018

[19] R. Jiang, H. Taghizadeh, and S. M. S. Hussain, "Smart meter data analytics for electricity theft detection," Electric Power Systems Research, vol. 189, pp. 106687, 2020.

[20] N. Lu, Y. Xie, and S. Chen, "Real-time monitoring and anomaly detection in smart grids using IoT," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9971–9982, Oct. 2020.

[21] A. S. Rajput and S. Patil, "Design of low-cost IoT based energy monitoring and theft detection system," International Journal of Electrical and Computer Engineering, vol. 11, no. 3, pp. 2321–2330, 2021.

[22] P. Kumar, R. Singh, and A. Verma, "Time-of-use based load analysis for electricity theft detection," Journal of Electrical Engineering & Technology, vol. 15, no. 5, pp. 2191–2200, 2020.