Scientific paper
Manuscript received March 30, 2026; revised May 26, 2026; accepted June 3, 2026

Journal of Energy

VOLUME 75 Number 2 | 2026

journal homepage: http://journalofenergy.com/

Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tuseef Ahmed Khan

Summary **— In today's world, as electricity demand continues to rise, one of the major challenges faced by power utilities is power theft. This not only results in significant revenue losses but also strains the power infrastructure, leading to inefficiencies and potential outages. Addressing this issue has become a critical priority for utility companies and governments. This project develops an IoT-enabled, LoRa-based power theft detection system that monitors electricity usage in real-time to identify unauthorized consumption. The system uses two ESP32 microcontrollers, two SCT013B current sensors, a ZMPT101B voltage sensor, and LoRa communication modules. These components are deployed in two setups: the Pole Side Setup and the Home Side Setup (Rx). The Pole Side Setup, placed at the electricity pole, includes an ESP32 microcontroller, an SCT013B current sensor, and a LoRa module. It measures the current flowing through the electrical line and wirelessly transmits this data to the Home Side Setup. The Home Side Setup, located at the consumer's premises, uses another ESP32, an SCT013B current sensor, a ZMPT101B voltage sensor, and a LoRa module. This setup compares the pole's transmitted current with the local current and voltage readings to detect discrepancies that might indicate theft. If unauthorized consumption is identified (e.g., when the pole's current exceeds the home's), the system logs the event and transmits the data to a Google Spreadsheet for easy monitoring. This provides utility companies with real-time alerts and detailed logs for quick response and analysis. The LoRa technology ensures long-range, low-power communication, making this system especially suitable for rural or remote areas where wired communication is impractical. The solution reduces manual inspections and operational costs by automating theft detection and offering real-time insights into electricity usage. In the future, the system can be enhanced by improving data security, integrating with smart meters, and expanding its coverage. The project represents a scalable, cost-efficient approach to combating electricity theft and optimizing power distribution.**

Keywords **— ESP32 microcontroller, Internet of Things (IoT), LoRa communication, Smart energy metering, Voltage sensor, Current transformer, Power theft detection, Real-time monitoring**

(Corresponding author: Raja Masood Larik)

Samandar Khan Afridi, Yasir Ali and Raja Masood Larik are with the Department of Electrical Engineering, NED University of Engineering and Technology, Karachi, Pakistan (email: rmlarik@neduet.edu.pk)

Zeeshan Ahmad Arfeen is with the Electrical Power Engineering Department, The Islamia University of Bahawalpur. Pakistan

Tauseef Ahmed Khan is with the Power and Water Utility Company for Jubail and Yanbu, Marafiq, Saudi Arabia

I. Introduction

The energy sector in Pakistan plays a crucial role in supporting national economic development and ensuring societal well-being. However, the sector continues to face persistent challenges, including inadequate infrastructure, supply–demand imbalances, and inefficiencies in energy consumption. These issues have created a pressing need for modernized energy management solutions that enhance operational efficiency and promote sustainability. Conventional energy metering systems have proven insufficient in addressing these challenges due to several inherent limitations. Traditional meters generally lack the capability for real-time monitoring, detailed data acquisition, and remote accessibility [1], which restricts the ability to analyze consumption trends and respond promptly to irregularities [2]. Manual meter reading further introduces human error, leading to inaccurate billing and inefficient energy utilization [5]. The maintenance and large-scale deployment of these systems are both resource-intensive and costly.

Pakistan's energy distribution network also experiences significant losses due to transmission inefficiencies, technical faults, and widespread electricity theft [4]. These issues reduce the financial sustainability of utility providers and compromise overall grid reliability. To address these problems, the implementation of advanced technological solutions has become essential.

This section reviews prior work relevant to IoT-based energy metering, long-range wireless telemetry, and automated power-theft detection. Each cited work is described succinctly to highlight methods, technologies, and findings that motivated the present prototype.

In [1], an ESP32-based electric energy consumption meter is presented; the work demonstrates feasibility of low-cost microcontroller platforms for real-time measurement and cloud-enabled logging of voltage, current, active power, and cumulative energy. In [2] reports an IoT energy-monitoring prototype that leverages a Wi-Fi microcontroller and MQTT-style data forwarding to achieve remote accessibility and basic dashboarding for voltage and current metrics. The prototype in [3] implements a postpaid electricity and water usage monitoring system, showing practical integration of utility metering with remote billing and monitoring workflows. In [4], an IoT prototype for smart home automation is presented, illustrating how distributed sensors and actuators can be integrated into a single management framework for residential energy control. Work in [5] develops a smart energy meter that compares grid and solar generation, demonstrating multi-source metering and cost-analysis capabilities for hybrid energy systems. The comparative study in [6] analyses the working principles of the ESP32 and other low-cost microcontrollers, providing perfor-

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

mance and suitability guidance for embedded IoT metering applications. Reference [7] document software tooling and IDE usage (Arduino IDE) for rapid firmware development and deployment in embedded IoT projects.

Long-range, low-power telemetry and its application to energy monitoring are addressed in several studies. In [8], a LoRa-based IoT system for industrial energy consumption monitoring is described, emphasizing reliable long-distance telemetry in harsh environments. The viability of LoRa-based networks for theft detection and wide-area monitoring is further examined in [9], which evaluates LoRa network design and performance metrics specific to energy-theft applications. The benefits of integrating LoRa with IoT sensing for enhanced power monitoring are discussed in [10], focusing on improved coverage and resilience. LoRa-based frameworks for rural energy monitoring are developed and benchmarked in [11] and [12], where network architecture and deployment trade-offs are explored. Multi-hop LoRaWAN designs for urban energy monitoring are proposed in [13], demonstrating methods to extend coverage in built-up areas.

Automated theft detection and analytics using IoT data streams are explored in [14] and [15]; these works outline system architectures and microcontroller-based detection mechanisms that reduce reliance on manual inspection. Challenges and taxonomy of theft-detection problems are summarized in [16], which identifies practical obstacles and operational constraints faced by utilities. Machine learning and deep-learning approaches for anomaly detection in energy consumption are surveyed and demonstrated in [17] and [18], where feature extraction and classifier design are used to improve detection accuracy and reduce false positives. Real-time analytics architectures for smart grids that incorporate streaming data processing and anomaly detection are presented in [19].

Security, data integrity, and tamper-evidence are addressed by blockchain and secure-framework studies. In [20], a blockchain-enabled smart energy meter architecture is proposed to provide tamper detection and immutable logging of meter readings. The combination of LoRa with blockchain for secure, decentralized energy monitoring is explored in [21], showing how distributed ledgers can augment trust in wide-area IoT deployments. Fog and edge computing strategies to reduce latency and enhance local detection while preserving cloud connectivity are discussed in [22], which proposes architectures that place computation closer to the meter for faster theft detection and reduced network load.

Reviews and infrastructure-level perspectives complement system-level studies. An overview of advanced metering infrastructure (AMI) and smart-grid communication requirements is provided in [23], framing interoperability and scalability challenges. Integration of next-generation cellular (5G) connectivity with IoT for low-latency energy monitoring is analyzed in [24], highlighting potential gains in responsiveness for critical grid applications. Finally, comparative and implementation-focused works such as [11], [12], and [10] collectively provide practical guidance on selecting radio hardware, network topology, and deployment strategies for large-scale monitoring.

The surveyed literature collectively demonstrates that low-cost microcontrollers (ESP32/ESP8266), LoRa/LPWAN communications, cloud analytics, and ML-based anomaly detection form a viable technology stack for scalable energy monitoring and theft detection. However, gaps remain in (i) practical end-to-end prototypes that combine non-invasive sensing, LoRa telemetry, cloud logging, and real-time ML inference in a single, field-tested package; (ii) lightweight yet secure data-integrity mechanisms suited to constrained LoRa payloads; and (iii) systematic field evaluations that quantify detection accuracy, communication reliability, and power/maintenance trade-offs across rural and urban deployments. These gaps motivate the current work, which integrates ESP32-based sensing, LoRa RA-02 telemetry, cloud logging (Google Sheets), and rule-based theft detection into a compact prototype aimed at validating feasibility, range, and detection performance under realistic conditions.

In Pakistan, the effective management of energy resources poses significant challenges due to outdated monitoring methods and inefficient data-handling processes. Traditional approaches to energy meter data monitoring often involve manual entry, leading to inaccuracies, delays, and limited insights into energy consumption patterns. This manual approach hampers decision-making processes and undermines efforts to optimize energy usage, reduce costs, and promote sustainability.

A. Comparative analysis with Existing IoT-Based Power Theft Detection System

To evaluate the significance and practical contribution of the proposed system, a comparative analysis was conducted with previously reported IoT- and LoRa-based power theft detection approaches available in the literature. Table 1 summarizes the comparison in terms of communication technology, cloud integration, theft detection capability, monitoring functionality, deployment suitability, and overall system complexity.

Table: i
Comparative Analysis of Proposed System with Existing Approaches

Reference	Communication Technology	Cloud Monitoring	Theft Detection Method	Real-Time Monitoring	Long-Range Communication	Deployment Cost	Key Limitation
Ref. [9]	LoRa	No	Current threshold comparison	Partial	Yes	Moderate	Limited cloud integration
Ref. [14]	Wi-Fi	Yes	Smart meter monitoring	Yes	No	Moderate	Short communication range
Ref. [15]	GSM/Wi-Fi	Partial	Raspberry Pi-based monitoring	Partial	Limited	High	Higher system complexity
Ref. [17]	Smart Grid Network	Yes	Deep neural network	Yes	Depends on infrastructure	High	Computational complexity
Ref. [18]	Smart Grid Network	Yes	Deep reinforcement learning	Yes	Depends on infrastructure	High	Requires large datasets
Proposed System	LoRa + Wi-Fi	Yes	Dual-side current comparison	Yes	Yes	Low	Fixed-threshold limitation

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

This research contributes directly to several United Nations Sustainable Development Goals (SDGs) by promoting innovation, sustainability, and transparency in energy management. It supports SDG 7 (Affordable and Clean Energy) by enhancing the accuracy and efficiency of energy metering to minimize losses due to theft, and SDG 8 (Decent Work and Economic Growth) through the creation of opportunities in the technology and energy sectors. The integration of IoT and LoRa technologies aligns with SDG 9 (Industry, Innovation, and Infrastructure) by fostering resilient and intelligent energy systems, while SDG 11 (Sustainable Cities and Communities) is addressed through improved access to reliable electricity and efficient urban energy management. Furthermore, the system promotes SDG 12 (Responsible Consumption and Production) by encouraging efficient energy use, and SDG 16 (Peace, Justice, and Strong Institutions) by ensuring transparency, accountability, and fairness in energy distribution and monitoring.

Main objective of the research:

- To develop an IoT-based system for monitoring energy meter data.
- To implement a theft detection mechanism.
- To test and verify the complete prototype system.

The present research introduces an Internet of Things (IoT)-based energy monitoring and theft detection system designed to overcome the limitations of conventional metering infrastructure. The proposed framework employs an ESP32 microcontroller integrated with current and voltage sensors to facilitate real-time data acquisition, analysis, and remote accessibility. The system utilizes secure communication protocols and data encryption techniques to ensure accurate, reliable, and tamper-resistant energy monitoring. This approach provides an efficient, low-cost, and scalable solution aimed at improving transparency, optimizing energy usage, and mitigating electricity theft in Pakistan's power sector.

II. Research Methodology

The research methodology is designed to ensure a systematic, structured, and efficient execution of each project phase to meet the defined objectives. The process began with the system design phase, where the overall architecture was developed to enable real-time monitoring of electrical energy consumption and wireless transmission of data to a centralized cloud platform using Google Sheets. The architecture incorporated core components, including the ESP32 microcontroller, SCT013B current sensors, ZMPT101B voltage sensor, LoRa RA-02 communication modules, and a cloud-based data storage interface for real-time analysis and visualization. Component selection was carried out based on factors such as performance efficiency, compatibility, cost-effectiveness, and reliability. The ESP32 microcontroller was chosen for its powerful dual-core processing capabilities, built-in Wi-Fi and Bluetooth functionalities, and seamless interfacing with analog and digital sensors. The LoRa RA-02 module was selected for its long-range, low-power communication characteristics, making it ideal for wide-area monitoring and data transmission in distributed energy systems. The SCT013B current sensors and ZMPT101B voltage sensor were integrated for accurate, non-invasive measurement of current and voltage, ensuring safety and ease of installation.

Following the design and selection stages, hardware development was carried out by assembling all components onto a custom-designed printed circuit board (PCB). The current and voltage sensors were interfaced with the ESP32 microcontroller for continuous data acquisition, while the LoRa module facilitated long-distance wireless communication between the pole-side and home-side units. To protect the components from environmental exposure and mechanical damage, the assembled circuit was enclosed in a weather-resistant casing. Software development was conducted using the Arduino Integrated Development Environment (IDE), enabling efficient communication between the sensors, microcontroller, and cloud database. The ESP32 microcontroller was programmed to read real-time current and voltage data, process the acquired measurements, and transmit them via the LoRa module to the receiver unit. The receiver unit, also based on the ESP32, was configured to receive the transmitted data, perform comparative analysis between the pole and home readings, and upload the processed information to Google Sheets through Wi-Fi connectivity. This configuration enabled automatic cloud logging, remote monitoring, and theft detection based on discrepancies between transmitted and received data.

Upon successful integration of hardware and software components, the complete prototype underwent comprehensive testing and validation to ensure functional accuracy and system reliability. The system was evaluated under multiple operational scenarios, including no-load, normal load, and simulated theft conditions. The performance of the prototype was compared with conventional energy meters to validate accuracy and consistency. The communication performance of the LoRa modules was examined by varying the distance between transmitter and receiver units to confirm long-range stability and data integrity. The testing phase provided valuable feedback for refining system calibration, optimizing sensor response, and improving transmission reliability.

The data collected during experimental testing were analyzed to identify anomalies, communication delays, or measurement deviations. Based on the analytical results, iterative adjustments were implemented in both the hardware and software to enhance precision, reduce latency, and improve real-time responsiveness. The processed data also provided meaningful insights into energy consumption behavior, supporting efficient load management and theft detection strategies. The adopted methodology ensured the development of a robust, scalable, and cost-effective IoT-based prototype capable of real-time monitoring and automatic detection of unauthorized energy consumption. The integration of LoRa-based communication, cloud data management, and non-invasive sensing technologies resulted in a reliable solution for enhancing transparency, operational efficiency, and sustainability within modern energy distribution networks.

A. Working Principle

The working principle of the IoT-based Reading Monitoring and Theft Detection Mechanism is grounded in the seamless integration of real-time energy monitoring, wireless communication, and advanced theft detection technologies. The system operates by continuously collecting data from electrical circuits using specialized sensors connected to an ESP32 microcontroller. These sensors, which measure both current and voltage, are strategically positioned to monitor energy consumption across various circuits. The ESP32 microcontroller acts as the brain of the system, processing the incoming data to calculate power usage. But this system doesn't just stop at monitoring; it's also designed to detect any anomalies that might indicate unauthorized energy use. By analyzing fluctuations in current and voltage, the system can identify patterns that suggest theft, such as sudden spikes in energy consumption or irregular power draws that deviate from normal usage. Once the data is processed, it's prepared for transmission through a LoRa RA-02 module, chosen for its ability to send data over long distances with minimal power consumption. This wireless transmission capability is crucial for ensuring that the data reaches a centralized server or cloud platform, where it can be securely stored and accessed by users in real time. The system's design allows for a responsive approach to theft detection; if any suspicious activity is

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

detected, an immediate alert is generated and transmitted as a priority signal. This proactive feature ensures that users can respond quickly to potential energy theft, minimizing losses and enhancing overall security. On the receiving end, another ESP32 microcontroller is responsible for processing the incoming data and uploading it to a Google Spreadsheet cloud via a Wi-Fi connection. This cloud-based storage solution not only secures the data but also makes it accessible from virtually anywhere, allowing users to monitor their energy consumption and any potential theft attempts through a web interface, smartphone, or laptop. The system's user interface is designed to be intuitive, providing clear visualizations of energy usage patterns and highlighting any detected anomalies. Furthermore, the system is built with scalability in mind. It can be easily expanded to monitor additional circuits or integrated with other IoT devices, making it versatile enough to adapt to different environments, whether residential or commercial. This flexibility is complemented by the system's robust data handling capabilities, with cloud storage ensuring that even large volumes of data can be managed efficiently. In essence, this IoT-based mechanism not only empowers users with real-time insights into their energy consumption but also equips them with the tools needed to detect and prevent energy theft, ultimately contributing to more efficient and secure energy management practices.

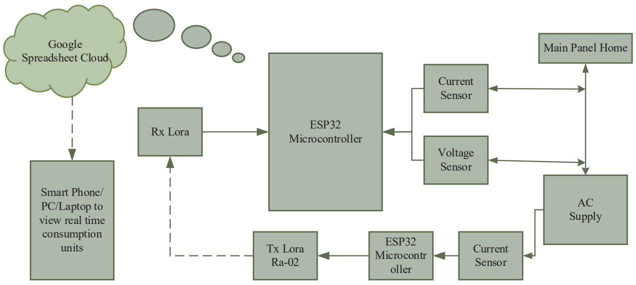


Fig. 1. Block diagram of the Prototype Development Project

Figure 1 is the block diagram of the prototype development of the project. The main controller is ESP32 with sensors that help with reading monitoring and detecting theft.

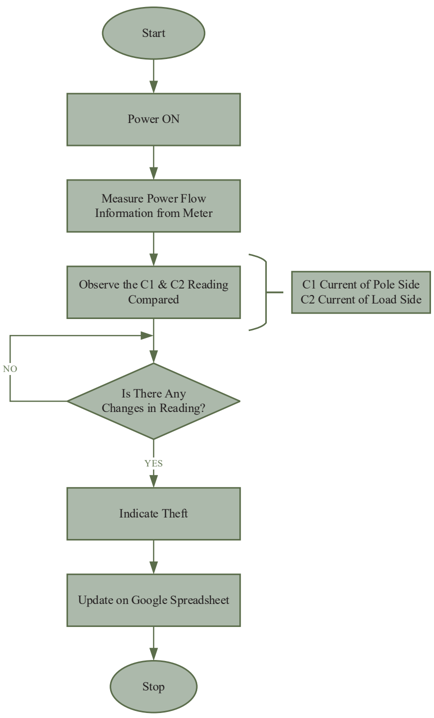


Fig. 2. Project methodology flow chart

The flowchart in Figure 2 outlines the process of detecting energy theft in an IoT-based monitoring system. It begins with powering on the system, which then measures the power flow from the meter by capturing the current values on both the pole side (C1) and the load side (C2). These readings are continuously observed and compared to detect any discrepancies. If the system finds no significant difference between C1 and C2, it continues monitoring without further action. However, if a change is detected, indicating a possible theft, the system flags this as a theft event. The incident is then logged and updated on a Google Spreadsheet for remote monitoring and record-keeping. The process is designed to loop continuously, ensuring real-time monitoring and quick detection of unauthorized energy use.

B. ESP32 Microcontroller

The ESP32 microcontroller (shown in Figure 3) functions as the core processing unit, handling data collection from connected sensors and wireless communication. The sensors are connected to GPIO pins 33 and 34, where they continuously monitor parameters like current and voltage. Pin 34 is designated for reading the voltage sensor data, while Pin 33 captures readings from the current sensor.

The dual-core Tensilica Xtensa LX6 processor within the ESP32 efficiently handles multitasking, allowing it to process the incoming sensor data and manage communication protocols simultaneously. The built-in Wi-Fi is used to transmit data to cloud storage or a local network, enabling real-time monitoring. The Bluetooth functionality is available for low-power communication with nearby devices when required. In Table 1 shows specification of ESP32 microcontroller.

The ESP32 communicates with LoRa modules to send sensor readings wirelessly over long distances, making it essential for energy monitoring and theft detection.

Table I.
Specifications for ESP32 Microcontroller

Specification	SCT-013 Input Current
Input Current 0-30A AC	0-5A AC
Output Signal	DC 0-1 V
Non-linearity	2-3 %
Built-in sampling resistance (RL)	62 Ω Turn Ratio
Turn Ratio	1800:1 G
Resistance Grade	Grade B
Working Temperature	25 °C~+70 °C
Dielectric Strength	1000 V AC / 1 min 5 mA

Fig. 3. ESP32 Microcontroller

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

C. SCT-013 Current Transformer

The SCT-013 (shown in Figure 4) is a non-invasive AC sensor that plays a key role in this project. It is used to measure up to 5A of alternating current (AC) by utilizing its split-core design, which allows it to clamp around live or neutral wires without the need for high-voltage rewiring. The current transformer (CT) in the sensor converts the AC flowing through the primary winding into a small, safe-to-handle current that flows through the secondary winding. In this project, the SCT-013 sensor is connected to the ESP32 microcontroller via GPIO pins 33. The specifications are mentioned in the Table 2.

The sensor continuously measures the AC current flowing through the monitored power lines, providing real-time data that the ESP32 processes and transmits wirelessly via LoRa to the monitoring system. The sensor's data is crucial for calculating energy consumption and detecting potential energy theft by analyzing current patterns.

Table II.
Specifications for SCT-013 Current Transformer

Specification	Details
Operating Voltage	2.2 to 3.6 V
GPIO Ports	3
ADC Ports	14
DAC Ports	2
Flash Memory	16 Mbyte
SRAM	250 Kbyte
Clock Speed	Up to 240 MHz
Wi-Fi	2.4 GHz
Sleep Current	2.5 μA

Fig. 4. SCT-013 Current Transformer

D. ZMPT101B AC Voltage Sensor

A high-precision ZMPT101B (shown in Figure 5) voltage transformer is the foundation of the ZMPT101B AC Single Phase voltage sensor module, which is used to detect precise AC voltage. With an ESP32 can be measure AC voltage quite effectively using this method. The analog output of the ZMPT101B sensor can be adjusted in response to the sensor's ability to measure voltage up to 250V AC. The specifications are mentioned in table 3. The module contains a multi-turn trim potentiometer for calibrating and adjusting the ADC output, and it is simple to use. In the prototype, the voltage signal is being measured and sent to the ESP32 microcontroller.

Table III.
Specifications for ZMPT101B Sensor

Specification	ZMPT101B Sensor
Output Signal	0-5v
Operating Voltage	DC 5V-30V
Measure within	250V AC.
Rated input current	2mA
Size	49.5 mm x 19.4 mm
Operating temperature	40ºC ~ + 70ºC

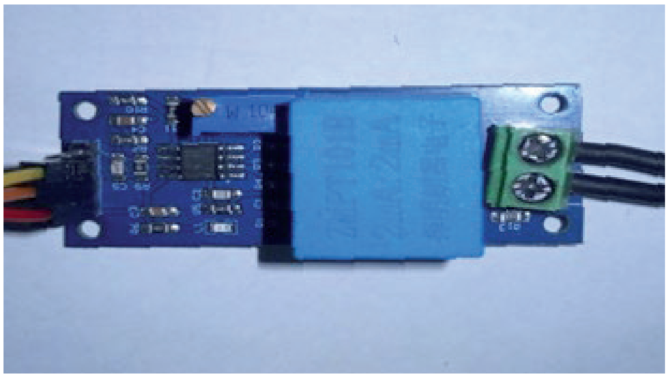


Fig. 5. ZMPT101B Sensor

E. LM2596 Buck Converter

The LM2596 (shown in Figure 6) power supply module is a step-down (buck) DC-DC converter designed to regulate voltage. It can efficiently handle loads of up to 3A while ensuring consistent regulation even when dealing with changes in input and output conditions. This module is available in different variants, offering fixed output voltages like 3.3V, 5V, and 12V, and it also includes an adjustable output version for flexibility. Notably, the LM2596 series operates at a switching frequency of 150 kHz, making it a versatile and adaptable choice for various applications. The characteristics are shown in Table 4. In this project, it has been used to convert 12V DC to 5V DC to give an input source to the desired components, such as relay module, BTS7960, esp32nodemcu controller, proximity sensor, and limit switches. The operating voltage of the system is 12V DC, so a converter is required for those components that can only operate at 5V to convert the input from 12V to 3.3V to provide a power source. Specifications of buck converters are given below.

Table IV.
Specifications of the LM2596 Buck Converter

Specification	Value
Model	LM2596 Buck Converter
Input Voltage Range	3.3V to 40V
Output Voltage Range	1.25V to 37V (adjustable)
Output Current	Up to 3A
Switching Frequency	150 kHz (typical)
Efficiency	Up to 92%
Output Ripple	50mV to 100mV (depending on load)
Load Regulation	±0.5%
Voltage Regulation	±2%
Operating Temperature	-40°C to +125°C
Dimensions	45 mm x 20 mm x 14 mm

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

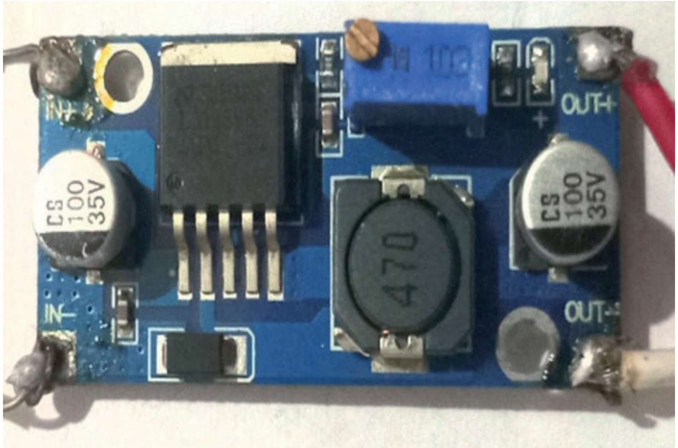


Fig. 6. Buck converter

F. Ra-02 Lora Module

The LoRa RA-02 (shown in Figure 7) module was utilized to enable long-range, low-power wireless transmission of current and voltage data from the energy meter to the central monitoring system. LoRa, an abbreviation for Long Range, is a low-power wide-area network (LPWAN) communication technology that facilitates data transmission over several kilometers, making it well-suited for distributed energy monitoring applications. The specifications are describes in Table 5. The RA-02 module serves as the primary medium for collecting data from the sensing units and transmitting it to the receiver node for analysis. This configuration provides continuous updates on energy usage and supports the detection of anomalies indicative of potential energy theft.

Table V.
Specifications of the Lora RA-02 module

Specification	Value
Module Model	Ra-02
Frequency Range	410-525MHz
Communication Range	Up to 10 km (in open areas)
Modulation	Lora Modulation Technique
Interface	SPI
Programmable bit rate	300Kbps
Antenna	IPEX
Max Transmit Power	18±1dBm
Power(Typical Values)	433MHz:TX:93mARX:12.15mAS-tandby:1.6mA 470MHZ: TX:97mARX:12.15mAStandby:1.5mA
Power Supply	2.5~3.7V Typical3.3V
Operating Temperature-	-40°C to +85°C
Weight	0.45g

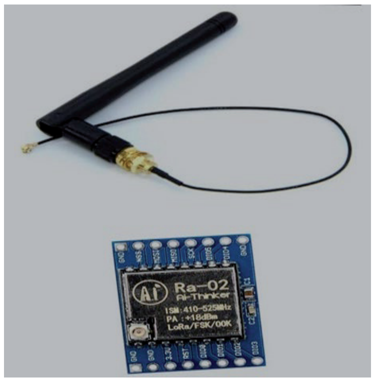


Fig. 7. Lora ra02 Module with Antenna

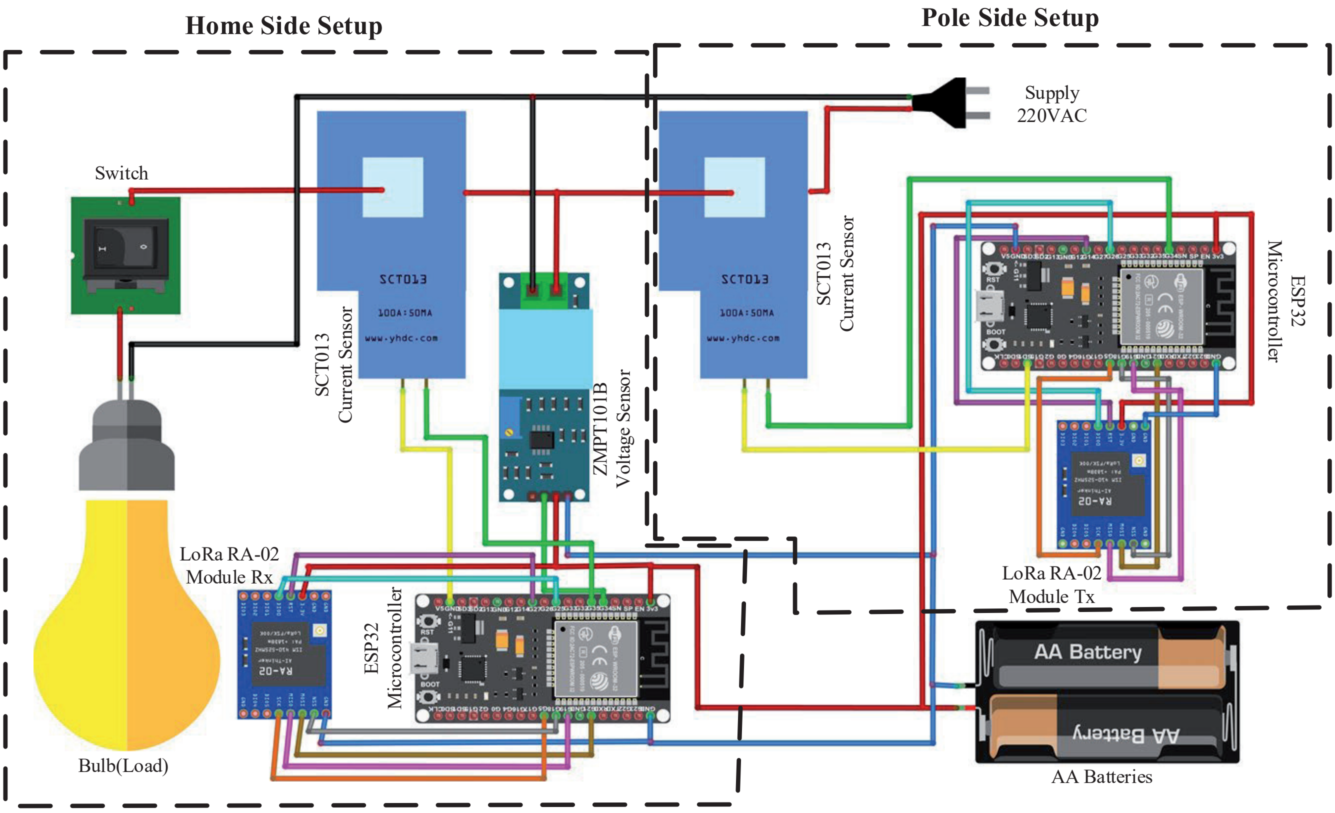


Fig. 8. Circuit Diagram of Project

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

The integration of LoRa technology minimizes the need for complex wiring infrastructure, thereby reducing installation costs and improving system scalability. Its strong resistance to interference and robust signal propagation ensure consistent data transmission even in challenging environments. Furthermore, the low power consumption of the RA-02 module enhances the operational efficiency of the system, allowing long-term, maintenance-free deployment in remote or rural areas.

G. Hardware System Architecture

Figure 8 presents the complete circuit diagram of the proposed IoT-enabled power theft detection system. The design consists of two integrated units: the Pole-Side Setup and the Home-Side Setup, which communicate wirelessly using LoRa RA-02 modules. Both units are based on ESP32 microcontrollers, ensuring efficient data processing, wireless communication, and real-time synchronization of current and voltage measurements.

Pole-Side Setup: The pole-side unit serves as the primary data acquisition node. It comprises an ESP32 microcontroller, an SCT013B current sensor, and a LoRa RA-02 module. The SCT013B sensor measures the current flowing through the distribution line, generating an analog signal proportional to the load. This signal is processed by the ESP32, which converts it into digital form and transmits it wirelessly to the home-side unit via the LoRa module.

The entire circuit is enclosed within a protective casing and mounted on the distribution pole. The setup is powered by AA batteries for energy efficiency, and a manual switch is provided to control system operation. The pole-side unit continuously monitors the current flow and acts as the transmitting node, enabling reliable, long-range, low-power communication with the home-side receiver.

Home-Side Setup: The home-side unit functions as the receiver and analytical node of the system. It incorporates an ESP32 microcontroller, an SCT013B current sensor, a ZMPT101B voltage sensor, and a LoRa RA-02 module. The LoRa module receives current readings from the pole-side transmitter, while the local sensors measure the home's current and voltage in real time. The ESP32 compares the received and measured current values to detect discrepancies that may indicate unauthorized power consumption.

When a difference between the pole-side and home-side readings exceeds the predefined threshold, the system identifies this as a potential theft event. The data, including date, time, voltage, current, power, and theft status, are then transmitted to a cloud-based Google Spreadsheet for real-time monitoring and record keeping. The home-side setup also provides serial output for on-site diagnostics and verification.

This two-node architecture ensures synchronized data measurement, long-range wireless communication, and real-time cloud integration. The hardware–software co-design provides a robust, scalable, and low-cost framework for continuous energy monitoring and accurate power theft detection.

H. Software Used for Programming Microcontrollers

The Arduino Integrated Development Environment (IDE) (shown in Figure 9) was employed to program both ESP32 (NodeMCU) microcontrollers used in the prototype development of the project. The IDE was selected for its versatility, hardware compatibility, and integrated debugging environment, which facilitated efficient embedded system development. The software provides a comprehensive interface consisting of a code editor, compiler, message console, and serial monitor, enabling real-time code verification and communication diagnostics. All embedded programs, referred to as sketches, were developed and compiled within the IDE using the .ino file extension. The environment supports structured programming through syntax highlighting, search, and automated error detection features. Configuration of the development setup included the installation of ESP32-specific libraries via the Board Manager and the integration of required dependencies for LoRa communication and cloud connectivity. The serial monitor was utilized to validate data transmission between the ESP32, sensors, and cloud interface. The Arduino IDE's open-source flexibility and extensive hardware support enabled seamless coordination between hardware and software components, ensuring reliable data acquisition, processing, and real-time transmission for the IoT-based energy monitoring and theft detection system.

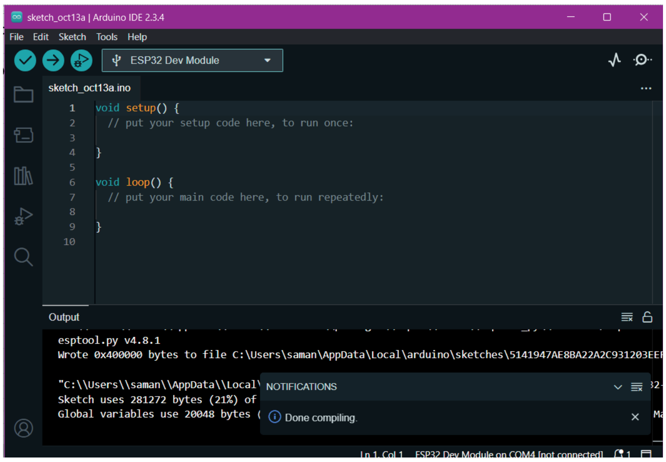


Fig. 9. Arduino IDE software

ESP32 with LoRa TX

The transmitter (pole-side) ESP32 microcontroller was programmed using the Arduino IDE to acquire current measurements from the SCT013B current sensor and transmit them via the LoRa RA-02 module. The program defines LoRa pin mapping according to ESP32 GPIO assignments to ensure proper communication between the devices. A correction factor was applied to calibrate sensor readings for improved accuracy. During initialization, the system configured the serial interface and LoRa communication module, halting operation if initialization failed. The main loop continuously read current values from the SCT013B sensor, applied the correction factor, and transmitted the calibrated data wirelessly through the LoRa link. Each transmission cycle included a short delay to prevent data congestion and ensure stable communication. This program enabled reliable long-range data transfer of current measurements from the pole-side setup to the receiver unit.

ESP32 with LoRa RX

The receiver (home-side) ESP32 combined Wi-Fi, LoRa, and sensor interfaces for real-time monitoring and data logging. The system established a Wi-Fi connection to transmit data to a Google Spreadsheet via HTTP GET requests, while simultaneously initializing LoRa for receiving current data from the transmitter. The ZMPT101B voltage sensor and SCT013B current sensor were configured to measure RMS voltage and current, respectively. Power and energy consumption were calculated by multiplying voltage and current values, with accumulated readings logged to

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

the cloud for continuous monitoring.

Incoming LoRa packets containing current readings from the pole-side setup were decoded and compared with local current measurements. If the difference between the transmitted and local current values exceeded a defined threshold, the system identified the event as potential theft and updated the theft status in the Google Spreadsheet. The program's functions ensured synchronized data acquisition, processing, and wireless communication, enabling accurate detection and real-time reporting of unauthorized energy usage.

Google Spreadsheet Integration and Interface

A Google Spreadsheet integrated with Google Apps Script was utilized for real-time data logging and visualization of energy parameters. The ESP32 microcontroller transmitted measured voltage, current, power, units, and theft status values to the cloud via HTTP GET requests. The Google Apps Script, deployed as a Web App, handled incoming requests, extracted parameters, and dynamically updated corresponding columns in the spreadsheet, enabling automatic data entry and confirmation of successful transmission. The real-time logging ensured accurate synchronization between the pole-side and home-side setups.

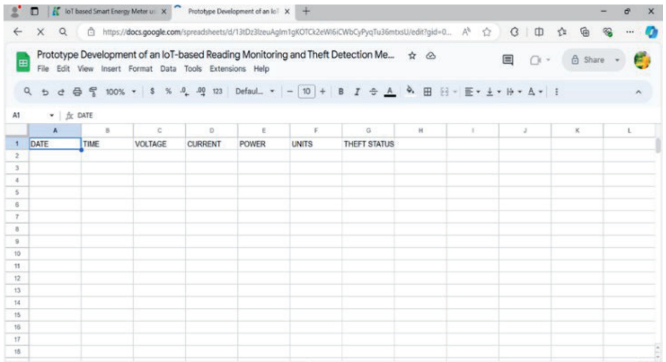


Fig.10. Google spreadsheets Interface

Figure 10 illustrates the Google Spreadsheet interface used for monitoring system performance. The spreadsheet automatically records parameters in structured columns date, time, voltage, current, power, units, and theft status allowing continuous observation and analysis. The integrated system architecture, comprising two ESP32 microcontrollers, two SCT013B current sensors, one ZMPT101B voltage sensor, and two LoRa RA-02 modules, was divided into a pole-side and a home-side setup. The pole-side module measured current at the distribution line and transmitted the readings wirelessly via LoRa to the home-side unit. The receiver simultaneously measured local voltage and current, comparing both datasets to identify discrepancies indicative of power theft.

All readings were continuously logged and visualized in the Google Spreadsheet, providing a reliable, cloud-based platform for real-time monitoring and record maintenance. This integration effectively combined IoT sensing, long-range communication, and cloud computing to achieve automated energy tracking and theft detection with high efficiency and accessibility.

I. Project Hardware Interface

The prototype comprises two primary units: the transmitter (pole-side) and the receiver (home-side). The pole-side unit, as shown in Figure 11, is enclosed within a circuit box mounted on the electricity pole and contains the complete electronic assembly, including the ESP32 microcontroller, SCT013B current sensor, and LoRa RA-02 communication module. This unit continuously measures the current flow and transmits the data wirelessly to the receiver module. The receiver side, depicted in figure 12, is installed at the consumer's premises and incorporates another ESP32, current and voltage sensors, and a LoRa module. This setup receives the transmitted data, compares it with the locally measured values, and identifies any discrepancies indicative of unauthorized power usage. Together, these interconnected units demonstrate the seamless integration of hardware and software components for efficient, real-time monitoring and theft detection within the proposed IoT framework.

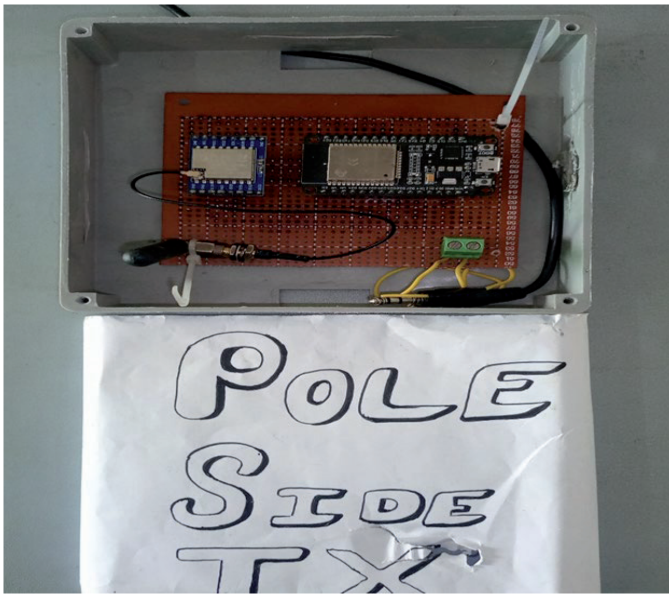


Fig. 11. Transmitter side

Fig. 12. Receiver side

3. Results and Discussion

The experimental evaluation of the proposed model was conducted (see table 6) to validate the performance and functionality of the developed IoT-based power theft detection system. Figure 13 presents the complete prototype used during testing. The system architecture comprises two primary modules: the Pole-Side Setup

https://doi.org/110.37798/2026752746

and the Home-Side Setup (Receiver). The pole-side configuration includes an ESP32 microcontroller, an SCT013B current sensor, and a LoRa RA-02 module enclosed within a protective circuit housing mounted on the distribution pole.

A. Quantitative Experimental Analysis

To evaluate the performance of the proposed IoT-based power theft detection system, multiple experiments were conducted under different operating conditions, including no-load, normal-load, and simulated theft scenarios. The measured parameters included voltage, pole-side current, home-side current, calculated power, current mismatch, and theft detection status.

The experiments were performed using a 220–230 V AC single-phase supply and a 200 W incandescent bulb as the test load. The current mismatch was calculated using:

$$\Delta I = \left|I_{pole} - I_{home}\right|$$

A theft condition was triggered when:

$$\Delta > 0.20$$

where 0.20 A was selected experimentally to avoid false triggering caused by sensor noise and minor load fluctuations.

Table VI
Experimental Results under Different Conditions

Test Condition	Voltage (V)	Pole Current (A)	Home Current (A)	Calculated Power (W)	Current Difference (A)	Theft Status
System OFF	0	0.00	0.00	0	0.00	No Theft
No Load	228	0.00	0.00	0	0.00	No Theft
Normal Load (200W Bulb)	227	0.88	0.85	193	0.03	No Theft
Theft Condition 1	226	1.34	0.82	185	0.52	Theft Detected
Theft Condition 2	229	1.52	0.91	208	0.61	Theft Detected

The current measurements obtained from the proposed system were compared with a conventional clamp meter to evaluate sensor accuracy.

The percentage error was calculated using:

$$\%\ Error = \frac{\left|I_{measured} - I_{reference}\right|}{I_{reference}} \times 100$$

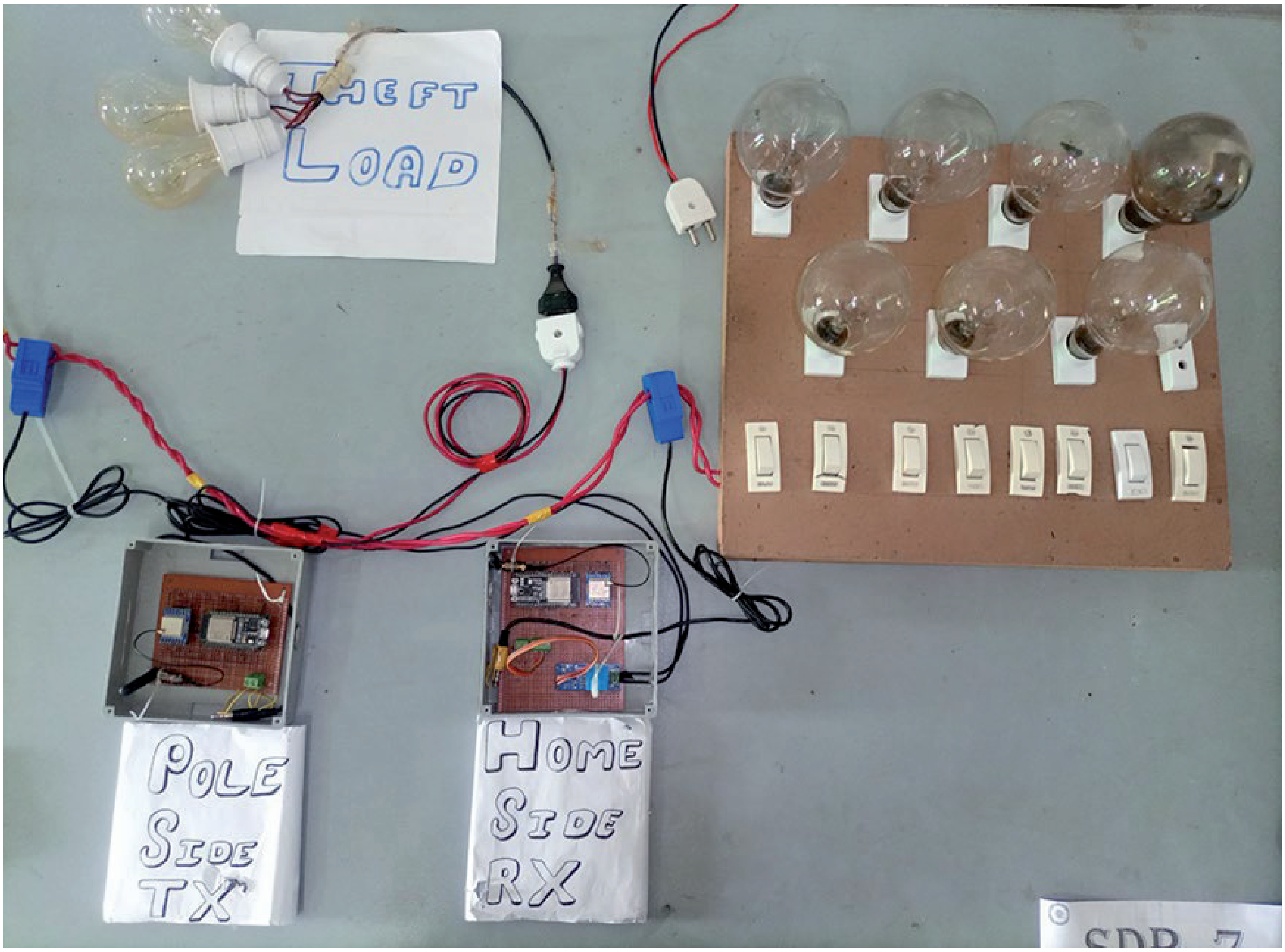


Fig. 13. Complete prototype of a project

https://doi.org/110.37798/2026752746

Table VII
Accuracy Comparison with Standard Meter

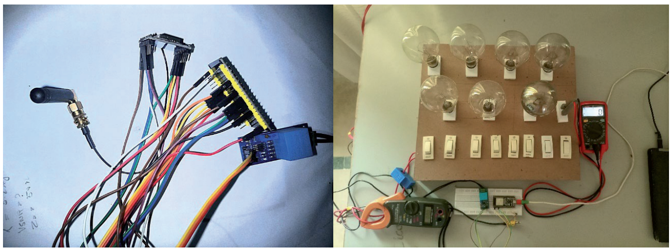
Load Condition	Prototype Current (A)	Reference Meter (A)	Error (%)
100 W Load	0.44	0.43	2.32
200 W Load	0.88	0.86	2.33
300 W Load	1.31	1.28	2.34

From conclusion of table 7 the average current measurement error of the ystem was approximately 2.33% demonstrationg acceptable accuracy for low-cost IoT-Based monitoring applications.

This unit measures the current flowing through the electrical line and transmits the acquired data wirelessly via the LoRa network. The home-side setup, equipped with another ESP32 microcontroller, an SCT013B current sensor, a ZMPT101B voltage sensor, and a corresponding LoRa module, receives the transmitted current readings and simultaneously measures local current and voltage values. The comparison between the transmitted and locally measured data enables real-time identification of discrepancies indicative of unauthorized energy consumption. The system performance was evaluated under four distinct operating conditions: (i) system off, (ii) system on with no load, (iii) normal load condition (200 W bulb), and (iv) theft condition.

B. Project off Condition

The implementation of the proposed power theft detection system was carried out using a combination of ESP32 microcontrollers, SCT013B current sensors, a ZMPT101B voltage sensor, and LoRa RA-02 communication modules. The observations and results obtained from these experiments are presented below.



(a) (b)

Fig. 14(a, b). When the system was off

Figure 14 (a, b) illustrates the system behavior when powered off. In this state, no data transmission occurred between the pole-side and home-side setups. The current sensors on both ends recorded zero readings, confirming the absence of current flow and verifying that the system remained in an idle, non-transmitting state. This baseline test established the accuracy and stability of the sensors and confirmed that the system operates only under active load conditions.

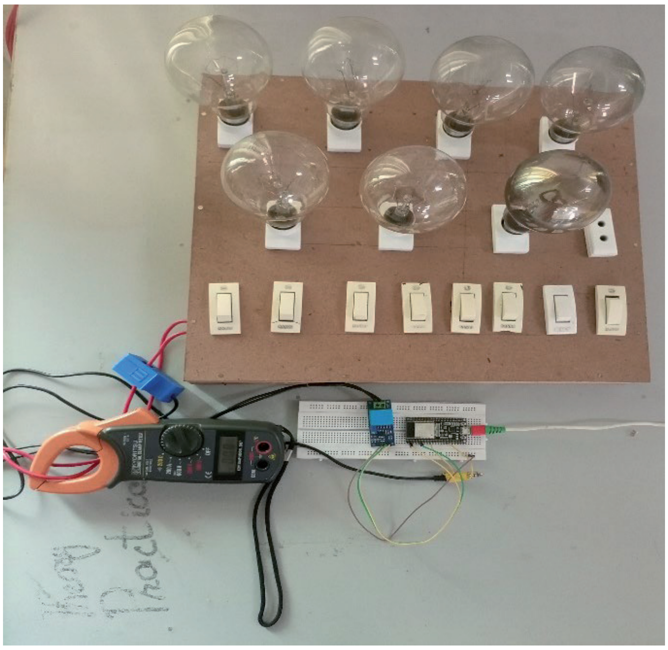
C. Project on Condition (No Theft)

Figure 15 (a, b) illustrates the system's operational state immediately after power-up. In this condition, the pole-side setup began measuring the current flow through the electrical line and transmitted the readings to the home-side setup via the LoRa RA-02 communication link. The communication reliability of the LoRa RA-02 modules was evaluated by increasing the separation distance between the transmitter and receiver units.

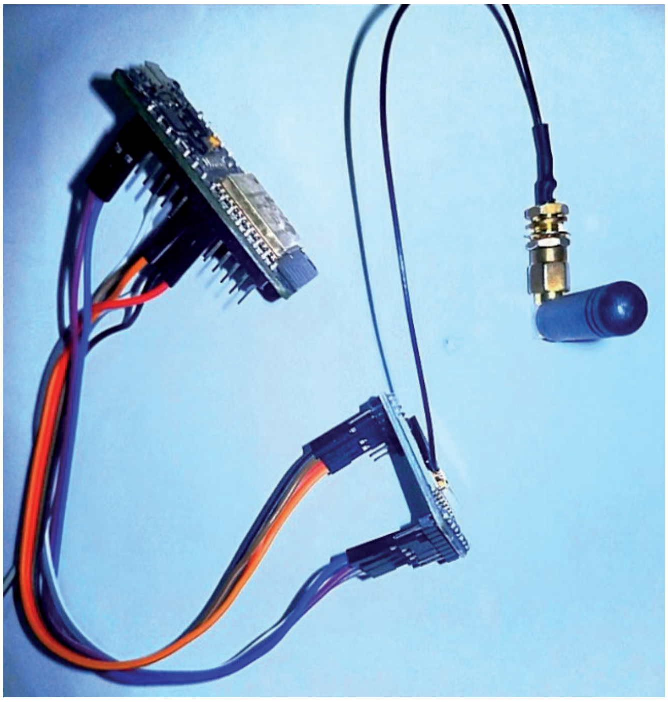
Table VIII
LoRa Communication Performance

Distance (m)	Packet Success Rate (%)	Average Delay (ms)
10	100	120
0	100	135
100	99	148
250	98	170
500	96	210

The table 8 results confirmed stable communication with minimal packet loss over moderate transmission distances, validating the suitability of LoRa technology for distributed energy monitoring application. The ESP32 microcontrollers on both sides successfully exchanged data, confirming that the wireless communication channel was functional.



(a)



(b)

Fig. 15. System on Condition

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746

As shown in Figure 16, during the no-load condition, the current readings on both sides remained zero, indicating no energy flow and verifying that the sensors were accurately calibrated. The results validated the system's stability, readiness, and ability to perform real-time monitoring without false detections under no-load or non-theft conditions.

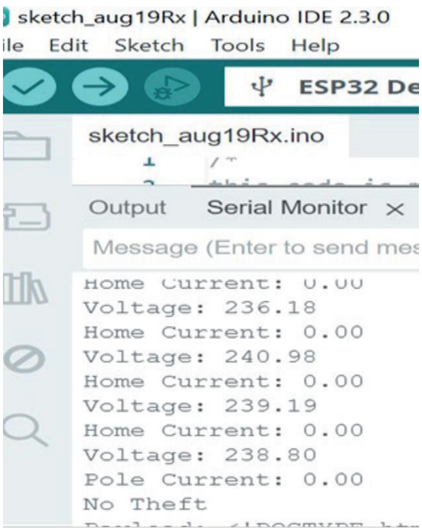
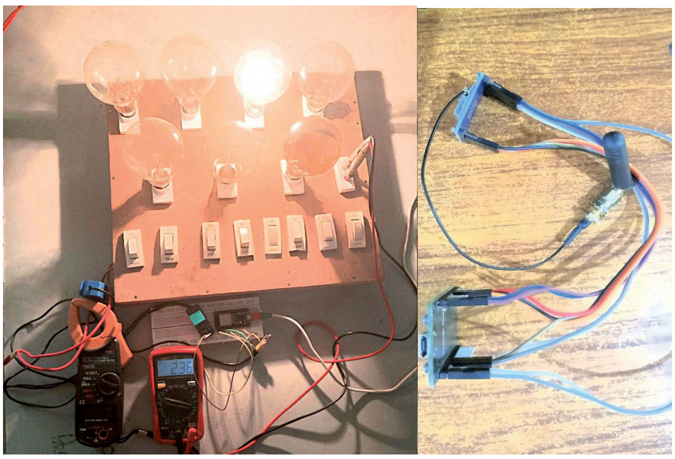


Fig. 16. No Theft

D. Project Normal Load Condition (200W Bulb, No Theft)

A 200W bulb was connected as the load in the experimental setup (see Figure 17(a, b)). The Pole Side Setup detected the current flow corresponding to the 200W bulb and transmitted this data to the Home Side Setup. The data received at the Home Side Setup was logged into the Google Sheet, written in columns, a,b,c,d,e,f, and g, respectively Date, time, voltage, current, power, units, and theft detection showing the expected readings based on the load.



(a) (b)

Fig. 17. Normal Load Condition (200W)

The system performed as expected under normal load conditions. The current sensor accurately measured the current corresponding to the 200W bulb, and the data was correctly transmitted and recorded. This result confirms that the system is capable of monitoring legal electricity usage and logging it for further analysis. The absence of theft detection alerts indicated that the system correctly identified this as a normal operating condition.

E. Theft Detected Condition

Figure 18 illustrates the system behavior under a simulated theft condition, where an unauthorized connection was created by tapping into the electrical line. During this scenario, the pole-side setup recorded an abnormal increase in current that did not correspond to the readings from the home-side setup. This discrepancy was automatically identified by the system as an anomaly. The data were transmitted to the home-side unit, where a theft alert was generated and logged in the cloud-based Google Spreadsheet for immediate visualization and record keeping.

Fig. 18. Theft Detected Condition

As shown in Figure 19, the serial monitor output confirmed successful detection of unauthorized energy usage. The system accurately identified the imbalance between transmitted and received current values, triggering the theft detection algorithm. The event was recorded in real time, providing clear digital evidence of the theft occurrence. These results validate the system's capability to detect, flag, and report unauthorized power consumption with high reliability and minimal latency, demonstrating its effectiveness for real-time monitoring and theft prevention applications.

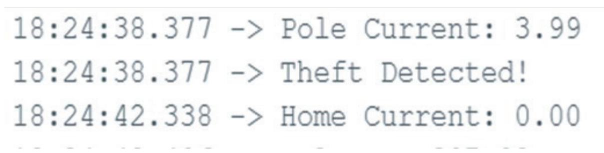
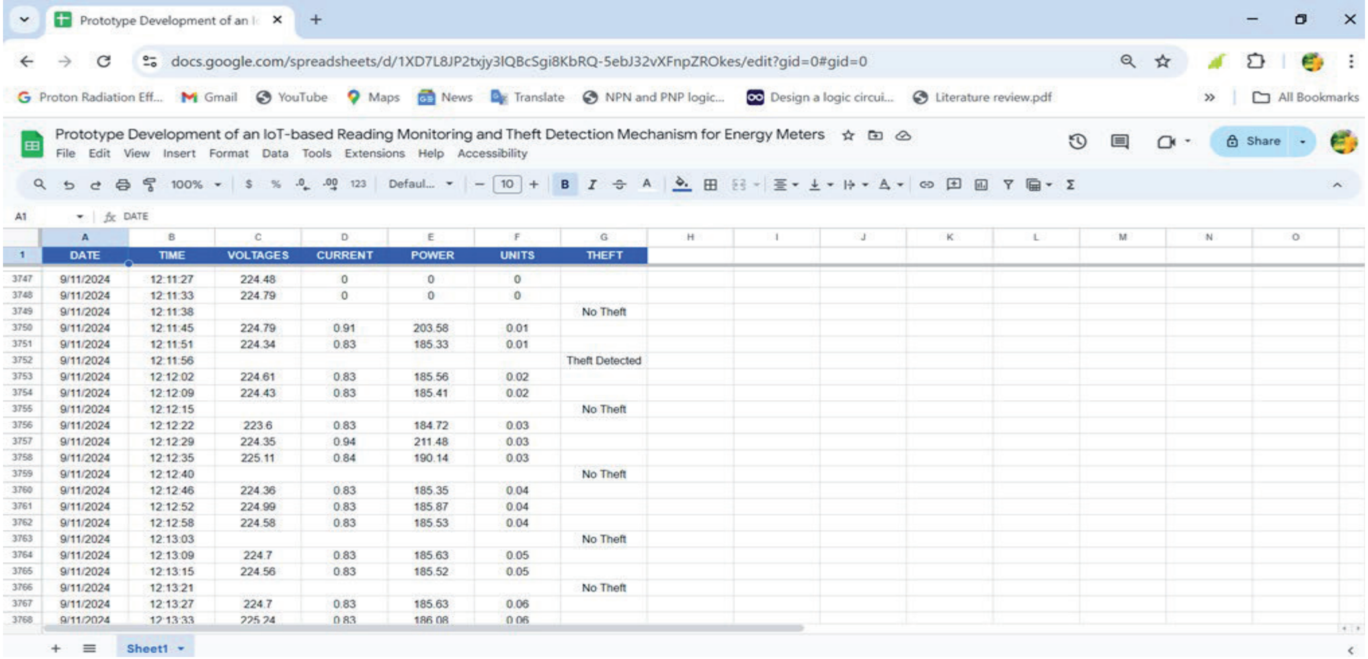


Fig. 19. Serial Monitor

F. Output on Google Spreadsheet

Figure 20 presents the Google Spreadsheet interface used for real-time data monitoring. The spreadsheet automatically updates with each transmitted data packet, displaying parameters such as date, time, voltage, current, power, energy units, and theft status. All readings are logged dynamically, ensuring accurate and continuous tracking of electricity consumption and system status.



Prototype Development of an IoT-based Reading Monitoring and Theft Detection Mechanism for Energy Meters

	DATE	TIME	VOLTAGES	CURRENT	POWER	UNITS	THEFT
3747	9/11/2024	12:11:27	224.48	0	0	0	
3748	9/11/2024	12:11:33	224.79	0	0	0	
3749	9/11/2024	12:11:38					No Theft
3750	9/11/2024	12:11:45	224.79	0.91	203.58	0.01	
3751	9/11/2024	12:11:51	224.34	0.83	185.33	0.01	
3752	9/11/2024	12:11:56					Theft Detected
3753	9/11/2024	12:12:02	224.61	0.83	185.56	0.02	
3754	9/11/2024	12:12:09	224.43	0.83	185.41	0.02	
3755	9/11/2024	12:12:15					No Theft
3756	9/11/2024	12:12:22	223.6	0.83	184.72	0.03	
3757	9/11/2024	12:12:29	224.35	0.94	211.48	0.03	
3758	9/11/2024	12:12:35	225.11	0.84	190.14	0.03	
3759	9/11/2024	12:12:40					No Theft
3760	9/11/2024	12:12:46	224.36	0.83	185.35	0.04	
3761	9/11/2024	12:12:52	224.99	0.83	185.87	0.04	
3762	9/11/2024	12:12:58	224.58	0.83	185.53	0.04	
3763	9/11/2024	12:13:03					No Theft
3764	9/11/2024	12:13:09	224.7	0.83	185.63	0.05	
3765	9/11/2024	12:13:15	224.56	0.83	185.52	0.05	
3766	9/11/2024	12:13:21					No Theft
3767	9/11/2024	12:13:27	224.7	0.83	185.63	0.06	
3768	9/11/2024	12:13:33	225.24	0.83	186.08	0.06	

Fig. 20. View electricity consumption on Google spreadsheet

4. Conclusion

The proposed IoT-enabled, LoRa-based power theft detection system represents a significant advancement toward efficient and reliable energy monitoring. The integration of ESP32 microcontrollers, SCT013B current sensors, a ZMPT101B voltage sensor, and LoRa communication modules enables accurate, real-time monitoring of power consumption at both the pole and consumer ends. The system's cloud-based data logging through Google Sheets facilitates continuous observation, rapid anomaly detection, and transparent record management for utility operators.

The experimental results validate the system's capability to detect power theft accurately by comparing current discrepancies between the pole-side and home-side readings. Under normal operating conditions, consistent current measurements confirm system reliability, while any deviation indicates unauthorized consumption. This automated detection mechanism minimizes manual inspection efforts and enhances the responsiveness of theft identification processes. The utilization of LoRa technology ensures long-range, low-power communication, making the system highly suitable for deployment in rural or remote regions where wired networks are infeasible. The cloud integration further improves accessibility and scalability, allowing utilities to monitor energy usage remotely and in real time.

The developed prototype provides a cost-effective, scalable, and energy-efficient solution for addressing electricity theft and improving grid reliability. Future enhancements will focus on incorporating artificial intelligence and cybersecurity frameworks to further strengthen system accuracy, resilience, and adaptability in smart grid environments.

5. Future Work

Future development of the proposed IoT-based energy monitoring and theft detection system will focus on the following key areas:

1. Employ artificial intelligence and machine learning algorithms to detect anomalies, predict power theft, and optimize energy usage patterns.
2. Implement advanced encryption and blockchain-based frameworks to ensure secure, tamper-proof data transmission within the IoT network.
3. Extend the system architecture for seamless integration with modern smart grid infrastructure and utility management systems.
4. Utilize 5G communication and edge processing to enable ultra-low latency, high-speed data handling, and real-time decision-making.
5. Develop user-oriented mobile and cloud platforms for remote monitoring, analytics, and control of energy systems.

6. Limitations

1. The proposed system employs a fixed-threshold current comparison method for theft detection, which may generate false-positive or false-negative results under dynamic load conditions and sudden current fluctuations.
2. The experimental validation was conducted under controlled laboratory conditions with limited load configurations; therefore, the results may not fully represent the complexity of large-scale real-world power distribution networks.
3. The performance of the system depends on stable LoRa communication and sensor calibration. Environmental interference, signal attenuation, and sensor drift may affect measurement accuracy and communication reliability.
4. The current prototype utilizes a rule-based detection mechanism and limited cybersecurity features, lacking advanced machine-learning algorithms, adaptive detection techniques, and robust data security frameworks for large-scale smart-grid deployment.

References

[1] P. S. Macheso and D. Thotho, "ESP32 Based Electric Energy Consumption Meter," International Journal of Computer Communication and Informatics, vol. 4, no. 1, pp. 23-35, 2022.

[2] K. Choorуang and K. Meekul, "Design of an IoT energy monitoring system," in 2018 16th International Conference on ICT and Knowledge Engineering (ICT&KE), 2018: IEEE, pp. 1-4.

https://doi.org/110.37798/2026752746

[3] M. Galina, M. W. Ramadhani, and J. W. Simatupang, "Prototype of Postpaid Electricity and Water Usage Monitoring System," in 2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC), 2019: IEEE, pp. 304-308.

[4] K. K. Rout, S. Mallick, and S. Mishra, "Design and implementation of an internet of things based prototype for smart home automation system," in 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), 2018: IEEE, pp. 67-72.

[5] M. Faisal, T. F. Karim, A. R. Pavel, M. S. Hossen, and M. H. Lipu, "Development of smart energy meter for energy cost analysis of conventional grid and solar energy," in 2019 international conference on robotics, electrical and signal processing techniques (ICREST), 2019: IEEE, pp. 91-95.

[6] H. Kareem and D. Dunaev, "The working principles of ESP32 and analytical comparison of using low-cost microcontroller modules in embedded systems design," in 2021 4th International Conference on Circuits, Systems and Simulation (ICCSS), 2021: IEEE, pp. 130-135.

[7] A. S. Ismailov and Z. B. Jo'Rayev, "Study of arduino microcontroller board," Science and Education, vol. 3, no. 3, pp. 172-179, 2022.

[8] M. Ahsan, M. A. Based, J. Haider, and E. M. Rodrigues, "Smart monitoring and controlling of appliances using LoRa based IoT system," Designs, vol. 5, no. 1, p. 17, 2021.

[9] A. K. SV, P. Kanakaraja, D. V. S. Prasad, T. G. Reddy, and N. Pardhasaradhi, "IoT Enabled LoRa based Power Theft Detection System," in 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022: IEEE, pp. 608-616.

[10] C.-S. Choi, J.-D. Jeong, I.-W. Lee, and W.-K. Park, "LoRa based renewable energy monitoring system with open IoT platform," in 2018 international conference on Electronics, Information, and Communication (ICEIC), 2018: IEEE, pp. 1-2.

[11] V. Križanović, K. Grgić, J. Spišić, and D. Žagar, "An advanced energy-efficient environmental monitoring in precision agriculture using LoRa-based wireless sensor networks," Sensors, vol. 23, no. 14, p. 6332, 2023.

[12] G. Y. Odongo, R. Musabe, D. Hanyurwimfura, and A. D. Bakari, "An efficient LoRa-enabled smart fault detection and monitoring platform for the power distribution system using self-powered IoT devices," IEEE Access, vol. 10, pp. 73403-73420, 2022.

[13] F. Ahmad, S. Mariyam, and F. Ahamad, "Smart city solutions: Enhancing infrastructure with LoRa multi-hop networks," in Emerging trends in computer science and its application: CRC Press, 2025, pp. 166-171.

[14] M. Jeffin, G. Madhu, A. Rao, G. Singh, and C. Vyjayanthi, "Internet of things enabled power theft detection and smart meter monitoring system," in 2020 International Conference on Communication and Signal Processing (ICCSP), 2020: IEEE, pp. 0262-0267.

[15] O. Darteh, "Design of internet of things based electricity theft detection using raspberry pi," 2021.

[16] X. Xia, Y. Xiao, W. Liang, and J. Cui, "Detection methods in smart meters for electricity thefts: A survey," Proceedings of the IEEE, vol. 110, no. 2, pp. 273-319, 2022.

[17] L. J. Lepolesa, S. Achari, and L. Cheng, "Electricity theft detection in smart grids based on deep neural network," Ieee Access, vol. 10, pp. 39638-39655, 2022.

[18] A. T. El-Toukhy, M. M. Badr, M. M. Mahmoud, G. Srivastava, M. M. Fouda, and M. Alsabaan, "Electricity theft detection using deep reinforcement learning in smart power grids," IEEE Access, vol. 11, pp. 59558-59574, 2023.

[19] M. U. Saleem, M. R. Usman, M. A. Usman, and C. Politis, "Design, deployment and performance evaluation of an IoT based smart energy management system for demand side management in smart grid," IEEE Access, vol. 10, pp. 15261-15278, 2022.

[20] M. Singh, S. Ahmed, S. Sharma, S. Singh, and B. Yoon, "BSEMS—a blockchain-based smart energy measurement system," Sensors, vol. 23, no. 19, p. 8086, 2023.

[21] C. Kumar and P. Chittora, "Integration of Blockchain Technology in Smart Grids for Enhancing Security, Efficiency, and Resilience: A Comprehensive Survey," in 2024 IEEE Third International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), 2024: IEEE, pp. 577-582.

[22] Z. A. Khan, M. Adil, N. Javaid, M. N. Saqib, M. Shafiq, and J.-G. Choi, "Electricity theft detection using supervised learning techniques on smart meter data," Sustainability, vol. 12, no. 19, p. 8023, 2020.

[23] O. Kebotogetse, R. Samikannu, and A. Yahya, "Review of key management techniques for advanced metering infrastructure," International Journal of Distributed Sensor Networks, vol. 17, no. 8, p. 15501477211041541, 2021.

[24] J. H. Shah, "5G-Enabled IoT Mesh for Real-Time Control and Predictive Maintenance," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 593-605, 2022.

Samandar Khan Afridi, Yasir Ali, Raja Masood Larik, Zeeshan Ahmad Arfeen and Tauseef Ahmed Khan, Empowering Smart Grids: An IoT and LoRa-Based Approach for Energy Monitoring and Theft Detection, Journal of Energy, vol. 75 Number 2 (2026), 27–39
https://doi.org/110.37798/2026752746