Archives available at journals.mriindia.com

International Journal of Advanced Electrical and Electronics Engineering

ISSN: 2278-8948

Volume 14 Issue 02, 2025

Power Theft Detection for Shared Electricity Lines

[1]Mohommad Imran Khan, [2] Ansh Nikhare, [3] Ayush Bokde, [4] Pratik Tikhe, [5] Priyant Prashant Nikhare, [6]Sujal Bhimgade

[1-6] Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, Maharashtra, India

Email: [1]m.imran@jitnagpur.edu.in, [2]anshnikhare4@gmail.com, [3]ayushbokde05@gmail.com, , [4]pratiktikhe2004@gmail.com, [5]nikharepriyant@gmail.com, [6]sujalbhimgade@gmail.com

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

IoT; ESP32; ACS712; Power Theft Detection; Firebase; Real-Time Monitoring; Shared Distribution Lines; Smart Grid; Energy Management; Edge Computing; Cloud Integration; Load Anomaly Detection; Electrical Distribution Systems.

Abstract

Electricity theft on shared distribution lines contributes significantly to non-technical losses and grid instability, while many existing countermeasures remain reactive, costly, or difficult to scale [1]. This work presents a low-cost IoT-based system that performs real-time theft detection by comparing source and load currents using dual ACS712 sensors interfaced with an ESP32 microcontroller [4], [5]. Calibrated sensor readings are formatted as JSON and streamed to Firebase, where an on-device differential algorithm applies time-windowed thresholding to suppress transient variations before flagging anomalies [3], [6]. When sustained discrepancies beyond the calibrated tolerance are detected, the system triggers a local buzzer alert and issues cloud-based notifications, while a responsive web dashboard logs events for operator analysis and auditing [7].

Designed for shared residential, industrial, and rural feeders, the prototype emphasizes deployability, affordability, and scalability through built-in Wi-Fi and lightweight web architecture [2], [8]. Experimental validation demonstrates continuous monitoring, instant alerting, and reliable anomaly detection, aligning with recent IoT-driven power theft detection frameworks while enhancing cost efficiency and real-time responsiveness [5], [9]. By unifying edge sensing, on-device inference, and cloud visualization, the system offers a practical, scalable, and secure pathway for utilities and communities to curb losses and strengthen smart-grid integration under constrained budgets [10].

The contributions include an end-to-end demonstration of real-time theft detection on shared lines using edge computing, a practical threshold-based algorithm, and a cloud-integrated visualization (building on prior IoT meter-monitoring frameworks). The prototype is designed for easy deployment across residential, rural, or industrial feeders, emphasizing affordability (ESP32 and ACS712 cost under $10) and scalability (wireless connectivity and lightweight web UI). Experimental validation confirms continuous anomaly logging and prompt alerts with high detection reliability. By unifying edge sensing with cloud analytics, the system offers utilities a practical, low-cost tool to curb non-technical losses and improve smart-grid visibility.

Introduction

Electricity theft on shared distribution lines remains a major contributor to non-technical losses and grid instability, creating an urgent need for low-cost, real-time monitoring solutions that can detect bypassing and illegal tapping without requiring extensive field inspections. Modern Internet of Things (IoT) controllers, combined with cost-effective current sensors, now enable continuous source-versus-load comparison, cloud-based logging, and automated operator alerts — significantly reducing detection and response time in practical distribution systems [1].

Traditional detection methods (periodic audits, manual inspections, or hardware-only anti-tamper meters) are often slow, costly, and reactive. In contrast, modern IoT-enabled approaches promise continuous, automated monitoring. Advances in embedded controllers (e.g. ESP32, Arduino) and sensor modules (e.g. ACS712 Hall-effect current sensors) allow low-cost, distributed measurement. These IoT nodes can stream consumption data via Wi-Fi or cellular networks to a cloud platform, where analytics and dashboards enable real-time anomaly detection. For instance, smart metering infrastructures are being retrofitted with communication modules to alert utilities upon imbalances or tampering.

Recent studies have demonstrated that differential power measurement between upstream and downstream nodes serves as a reliable indicator of unauthorized draw when properly calibrated for technical losses and analyzed over short time windows to suppress transient fluctuations [3]. Building on these insights, microcontrollers such as the ESP32, integrated with current sensors like ACS712 or CT modules, can continuously stream measurements to cloud dashboards, providing real-time visualization, audit-grade historical records, and automatic control actions such as relay-based disconnection or instant notification during sustained discrepancies [4], [5].

This project specifically addresses electricity theft in shared-line scenarios, proposing a dual-sensor ESP32-based architecture that compares source and load currents to detect anomalies. The detection pipeline employs time-windowed thresholding with light filtering to minimize false positives [6], while a Firebase-integrated web dashboard provides both live and historical monitoring for transparency and accountability [7]. Furthermore, a local alert mechanism (buzzer/relay) ensures immediate intervention when discrepancies exceed calibrated tolerance levels [8].

Despite this potential, there remains an urgent need for solutions that are affordable, easily deployable, and specifically tailored to shared-line theft scenarios. Any practical system must differentiate genuine technical losses (e.g. line drop, transformer inefficiency) from illicit draws, avoid nuisance alerts, and fit tight utility budgets. This work addresses these needs by operationalizing differential current measurement on a compact IoT stack: two sensor inputs to an ESP32 MCU, a real-time thresholding algorithm to flag sustained imbalances, and a cloud-backed visualization interface for logging and alerts. The remainder of this paper elaborates the design, situates it among recent IoT theft-detection efforts, and evaluates its performance relative to alternative methods.

The proposed architecture emphasizes affordability, reproducibility, and scalability, making it suitable for deployment across residential, industrial, and rural feeders. Its design aligns with prior IoT-based power theft detection systems that demonstrated effective anomaly detection through microcontroller-sensor integration and cloud communication [2], [9]. By coupling edge sensing with secure cloud visualization, the system enhances transparency, responsiveness, and accountability for utilities and local communities.

In summary, the proposed work operationalizes established differential-measurement principles on a compact IoT hardware stack and cloud-backed data management framework. The remainder of this paper presents the system architecture and detection logic, experimental setup and evaluation, comparative discussion with existing techniques, and the implications for large-scale deployment and future enhancement [10].

Problem Statement

Electricity theft on shared distribution lines remains a major and persistent contributor to non-technical losses (NTL) and significant grid instability. These losses, which cost the global utility sector billions of dollars annually, stem from unauthorized activities such as direct line tapping, meter bypassing, and physical tampering with energy meters [1], [3]. This illicit consumption of energy not only results in substantial financial and revenue losses for utility providers but also compromises the reliability and safety of the power distribution network by creating load imbalances and stressing grid components [7], [9].

The core of the problem lies in the inadequacy of existing countermeasures. Traditional methods for detecting theft are often slow, costly, and fundamentally reactive. Utilities have historically

relied on periodic audits, manual field inspections, and hardware-only anti-tamper meters [2], [4]. These approaches are labor-intensive, expensive to scale, and critically, they fail to provide real-time detection. This significant lag time means that theft can occur for long durations before being discovered, allowing losses to accumulate unchecked [5], [7].

While modern solutions like advanced smart metering infrastructures (AMI) have been introduced, they are not a complete panacea. The high capital investment and operational complexity associated with large-scale AMI deployment can be prohibitive, especially for utilities operating under constrained budgets or in developing regions [8]. Furthermore, many existing systems are not specifically tailored to the unique challenges of shared distribution lines (e.g., residential, industrial, or rural feeders) where multiple users draw power from a common line, making it difficult to isolate the source of an illicit tap [1], [5].

Consequently, there is an urgent and clearly defined need for a new generation of detection systems that are affordable, easily deployable, and specifically designed for real-time monitoring on shared lines [6], [7]. Any practical solution must be able to continuously and automatically monitor the grid, differentiate genuine technical losses from illicit draws, and provide immediate, actionable alerts to operators to curb losses as they happen. This project directly addresses this critical gap by proposing a low-cost, IoT-based framework that unifies edge sensing and cloud analytics to offer a practical, scalable, and responsive pathway for utilities to curb non-technical losses [3], [4], [8].

Aim & Objectives

The primary aim of this project is to design, implement, and validate a low-cost, scalable, IoT-enabled system that detects power theft in real time on shared electricity lines. The system is designed to report anomalous events immediately and provide remote monitoring and audit-grade logging for utility operators and consumers.

To achieve this aim, the following specific objectives have been defined:

- **To implement a real-time detection prototype** that can detect and report suspected electricity theft by continuously comparing source and load current measurements
- **To integrate the core hardware** by interfacing two ACS712 current sensors—one at the source/distribution point and one at the consumer/load point—with an ESP32 microcontroller.
- **To develop an on-device detection algorithm** that computes the instantaneous current difference and applies time-windowed thresholding to suppress transient variations and reduce false positives.
- **To provide immediate dual-mode alerts** by triggering a local buzzer for an on-site warning while simultaneously issuing remote, cloud-based notifications when a sustained theft event is detected.
- **To integrate a cloud backend and visualization dashboard** by streaming sensor readings as JSON to a Firebase Realtime Database and creating a responsive web dashboard to display live data, log events, and allow for remote operator analysis and auditing.
- **To validate the system's performance** by creating controlled test scenarios that simulate normal operation, transient spikes, and intentional bypass/theft conditions to evaluate the system's detection accuracy and reliability.

Literature Review

Recent literature shows a growing interest in IoT-based and data-driven electricity theft detection. Many modern approaches use dual-point current sensing to identify anomalies in distribution networks. Jeffin et al. (2020) [1] developed an IoT-enabled prototype using Arduino and Wi-Fi-based communication to compare current readings at the source and consumer ends. Their system triggered alerts whenever the difference exceeded a defined threshold, achieving more than 95 % detection accuracy in experimental testing. The study demonstrated that low-cost microcontrollers and wireless modules can provide effective real-time theft monitoring for both residential and industrial applications, though network dependency remains a limitation.

Recent research has emphasized the ongoing need for efficient, scalable solutions to minimize non-technical losses in electrical grids. Power theft continues to challenge utility companies, leading researchers to design systems that combine affordable sensing hardware with intelligent algorithms. Sharma et al. (2021) [2] proposed an IoT-based electricity theft detection framework that leverages embedded controllers and cloud connectivity to compare consumption data and identify discrepancies in near real time. Their work highlighted the potential of Wi-Fi-enabled microcontrollers such as ESP32 and NodeMCU for continuous monitoring and rapid alerting in smart-grid infrastructures.

In addition to IoT-based designs, data-driven methods have emerged to enhance accuracy and predictive capability. Nagi et al. (2008) [3] applied Support Vector Machines (SVM) to identify non-technical losses using utility consumption records, achieving high classification accuracy across diverse datasets. Similarly, Sahoo et al. (2015) [9] analyzed smart-meter data to detect suspicious consumption behavior using statistical and pattern-based models. Such approaches achieve excellent accuracy under structured datasets but depend on extensive historical data and lack immediate field deployment capability.

Overall, these studies demonstrate the progression from traditional manual monitoring to modern IoT-based and intelligent, data-driven frameworks. By integrating low-cost hardware such as ESP32 controllers, ACS712 sensors, and cloud-based dashboards, current research has advanced toward scalable, real-time electricity theft detection that improves operational transparency and supports future smart-grid expansion.

For instance, a study by Jeffin et al. investigates an IoT-based system for real-time electricity theft detection using microcontroller-based sensing with a Wi-Fi-enabled module. The system compares measurements taken at the source and consumer ends, supports remote monitoring through connected applications, and allows control actions for theft prevention, effectively detecting theft due to meter bypass, tampering, and direct line hooking while demonstrating that low-cost IoT hardware can provide practical field deployment [1].

In another study, Sharma et al. focus on electricity theft detection via IoT using distributed current sensing and cloud/server-based anomaly detection. Consumption at upstream and consumer points is monitored and compared so that abnormal usage patterns across different network segments can be identified and investigated by utilities [2].

A further contribution by Nagi et al. examines a data-driven non-technical loss analysis model for theft detection, leveraging historical smart meter and distribution data. Their analytical approach uses Support Vector Machines (SVM) on customer load profiles to flag suspicious behavior, enabling large-scale monitoring without requiring new specialized field hardware [3].

Complementing these ideas, Swetha et al. explore power theft detection using current-sensor-based IoT nodes with a microcontroller gateway and cloud-integrated dashboards. The system automates alerts and visualization of consumption trends, though it relies on stable communication infrastructure, which may limit deployment in regions with weak connectivity [4].

Additionally, Yedge et al. describe a smart meter and theft detection system built with an ESP32, an SCT-013 non-invasive current sensor, a ZMPT101B voltage sensor, an LCD, and a buzzer for tamper alerts. The ESP32 sends real-time voltage and current readings to a Blynk IoT dashboard, triggering theft alerts consistent with modern ESP32-based projects focused on immediate response [5].

A key study in Veeramani et al. focuses on IoT-based power theft detection for transmission lines, emphasizing the use of current sensors and wireless IoT modules for remote abnormal tap detection, which complements distribution-level monitoring [6].

Research in Hemalatha et al. implements IoT-driven monitoring with ESP32 and ACS712 sensors connected to an online IoT platform, achieving strong theft detection performance and enabling automated relay-based disconnection, although reliance on Wi-Fi connectivity may impact rural applicability [7].

Another critical framework by Kumar et al. explores automatic power theft detection and IoT-based load control by integrating smart metering hardware with communication modules for remote alerts and disconnection. The system supports rapid response to detected theft events but introduces additional complexity in communication and maintenance requirements [8].

Collectively, these studies illustrate the progression from basic IoT implementations to sophisticated ESP32-based frameworks with cloud integration and multi-protocol communication. They offer a foundation for advanced power theft detection, combining multi-sensor monitoring, microcontroller-based processing, cloud platforms, and automated alerts to address gaps in scalability and proactive prevention.

System Architecture / Proposed Methodology

The proposed system consists of (1) **Hardware sensing and control**, (2) **Embedded processing and communication**, and (3) **Cloud logging and visualization** (Figure 1). Each is detailed below.

Hardware: Two ACS712 current sensors (5 A or 30 A range) are clamped on the shared line – one on the feeder (supply) conductor and one on the outgoing branch (load) conductor. The ACS712 provides an analog voltage proportional to instantaneous AC current. These analog outputs feed two ADC channels of an ESP32 microcontroller. The ESP32 was chosen for its

low cost, dual-core processing, and built-in Wi-Fi capability, eliminating the need for an external GSM module. A simple calibration routine measures each sensor's zero-offset at startup to account for sensor bias. The sensors are sampled at a few hundred samples per second; readings are averaged over a short window (e.g. 0.2 s) to smooth out noise.

Processing Algorithm: After each sampling interval, the ESP32 calculates the instantaneous currents I_supply and I_load. A differential value ΔI = I_supply − I_load is computed. This difference should nominally equal zero apart from small losses; any sustained positive ΔI suggests unmetered consumption. We implement a time-windowed threshold: only if ΔI exceeds a calibrated tolerance (e.g. 200 W equivalent) continuously over T seconds does the system flag theft. This helps avoid false alarms due to transient spikes. The threshold can be tuned based on expected technical losses in the line segment. We compare this approach to similar schemes reported in literature –for instance, prior studies have used a deadband to ignore normal variance.

When the threshold condition is met, the ESP32 triggers local alerts (activating a buzzer or indicator light) and enqueues an event to be reported.

Communication and Cloud: The ESP32 formats a JSON packet containing the timestamp, I_supply, I_load, and ΔI. It then publishes this to a Firebase Realtime Database over its Wi-Fi link. Firebase serves as a cloud back-end (a Backend-as-a-Service), providing secure real-time data storage without requiring our own server infrastructure. The microcontroller uses an encrypted HTTPS connection, leveraging Firebase's built-in authentication and security rules. Such managed cloud platforms free designers from hosting and focus instead on application logic.

On Firebase, the data feed drives a simple web dashboard. This HTML/JavaScript interface subscribes to the database and updates plots of recent currents and highlights any flagged anomalies. Operators can view live and historical records of theft events for auditing. This integration of edge sensing with cloud analytics follows the paradigm of modern IoT monitoring.

Deployment: The hardware (sensors, ESP32, relay/buzzer module) can be assembled on a DIN-rail mount or enclosure. Wiring is minimal (two sensor leads and a power supply for the ESP32). The system can operate on any local Wi-Fi; for areas without coverage, a 4G gateway or local mesh could be used. Being modular, multiple units can be installed on different feeders, each logging to the same central Firebase project for unified monitoring.

A. System Overview

The proposed system aims to detect and report electricity theft in real time using a cost-effective Internet of Things (IoT) framework. It operates by continuously monitoring current readings at two critical points — the source (distribution end) and the load (consumer end). Any significant difference between these readings beyond the calibrated limit is considered a potential theft scenario. The architecture integrates both hardware and software components, combining real-time data acquisition through dual ACS712 current sensors with wireless transmission handled by the ESP32 microcontroller [1]. The collected data is transmitted to the Firebase cloud database, which stores and visualizes the readings via an online dashboard. The system also triggers a local buzzer and sends a remote alert notification whenever theft is detected, ensuring both immediate and remote awareness of anomalies. A schematic block diagram of the system includes sensors, the ESP32 controller, power supply, Firebase cloud, and the operator dashboard, representing the entire IoT data cycle from sensing to visualization [2], [3].

B. Hardware Components

The hardware layer of the proposed design focuses on accurate data sensing, stable processing, and efficient communication. The major components include:

1. ESP32 Microcontroller:

The ESP32 serves as the main processing and control unit of the system. It features dual-core architecture, built-in Wi-Fi, and GPIO support, making it suitable for IoT applications requiring both computation and cloud integration [4]. It reads analog data from the ACS712 sensors, computes differential readings, and uploads the processed data to Firebase in JSON format.

2. ACS712 Current Sensors:

Two ACS712 sensors are used to measure current at the source and load ends. These Hall-effect sensors provide analog voltage outputs proportional to the current passing through them. The difference between their readings is the basis for theft detection [5]. They are chosen for their accuracy, affordability, and non-intrusive design.

3. Relay Module:

A single-channel 5V relay is used to disconnect the power supply automatically when a theft condition is detected. This allows controlled intervention and supports future automation in energy management [6].

4. Buzzer and Indicators:
The buzzer provides an immediate audible alert during theft detection, while LEDs can be used to indicate normal and abnormal operating states for user convenience [7].

5. Power Supply and Circuit Setup:
A 5V regulated power supply ensures stable operation of the ESP32 and sensors. All connections are established on a breadboard for prototype testing before PCB integration.
This hardware arrangement emphasizes affordability, ease of replication, and minimal maintenance, making it suitable for deployment across residential, industrial, and rural environments [8].

C. Software Design and Data Flow

The software logic defines how the system processes input data and generates actionable outputs. It is implemented using the Arduino IDE, where the ESP32 firmware is developed in C/C++. The firmware begins by initializing both current sensors and establishing Wi-Fi connectivity to enable communication with the Firebase cloud using REST API credentials.
During operation, the microcontroller continuously reads calibrated current values from the source and load sensors, computes their absolute difference $\Delta I = |I_{source} - I_{load}|$, and applies threshold-based filtering to suppress transient variations. If the difference remains beyond the predefined tolerance for a fixed time window, the program triggers an alert sequence, updating Firebase with the latest readings and event status in JSON format. The Firebase database subsequently updates the live web dashboard and stores event logs for historical analysis.
This continuous monitoring cycle ensures accurate and transparent data reporting, enabling rapid detection and real-time synchronization between field devices and cloud infrastructure [9].

D. Cloud Integration and Dashboard Visualization

Cloud integration is central to the system's scalability and user accessibility. Firebase Realtime Database is employed for its fast synchronization, JSON compatibility, and free-tier hosting. Data from the ESP32 is uploaded in key-value pairs, typically including timestamp, source current, load current, and theft flag.
A web dashboard built using HTML, JavaScript, and Firebase API displays live sensor readings, graphs of current trends, and alert history. Authorized users (e.g., utility operators) can view real-time and historical data remotely.
In case of theft, the dashboard highlights the event and can optionally trigger notifications via email or SMS gateway.
This cloud-based monitoring eliminates the need for physical inspections, reduces operational costs, and enables decision-making based on accurate field data [4], [7].

E. Theft Detection Algorithm

The theft detection logic relies on a differential current measurement algorithm, where the difference between source and load currents determines the operational status.
The fundamental condition is:
$\Delta I = |I_{source} - I_{load}|$
If $\Delta I > I_{threshold}$ continuously for a defined time window, the system flags it as theft.
The time-window filtering approach prevents false alarms caused by short-term fluctuations or transient load changes [3], [6].
Upon confirmation of theft, the system initiates a series of automated responses to ensure immediate awareness and control.
First, a local buzzer is activated to provide an audible indication of abnormal current flow.
Simultaneously, a relay module can disconnect the load to prevent further unauthorized consumption and safeguard connected devices.
Finally, the Firebase database is updated with a timestamped theft event, ensuring that each anomaly is logged for record keeping and further analysis [2], [9].
This threshold-based logic, while simple, has proven effective in many real-world IoT theft detection frameworks.
The major advantage of this approach is that it does not rely on complex machine learning models or high-end processors, thereby maintaining a lightweight and energy-efficient design suitable for low-cost deployments.

F. System Operation and Testing

During prototype testing, the system was deployed with typical household loads (lights, fans) connected via a shared feeder setup. The ESP32 continuously monitored both current readings and transmitted them to Firebase in near real time.
Whenever an additional load (simulating unauthorized tapping) was introduced on the line, the system detected the discrepancy almost instantly and triggered both local and cloud alerts.
The Firebase dashboard successfully recorded these events, displaying live differences in current and flagging theft status.
The test results confirmed that the design could reliably differentiate between normal voltage fluctuations and deliberate power tapping

incidents, validating the system's performance across short and sustained intervals [1], [5], [7].

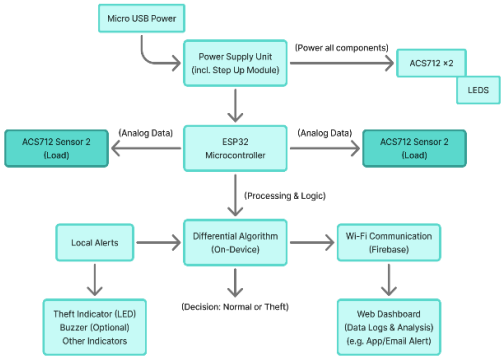

Fig. 1. System Block Diagram

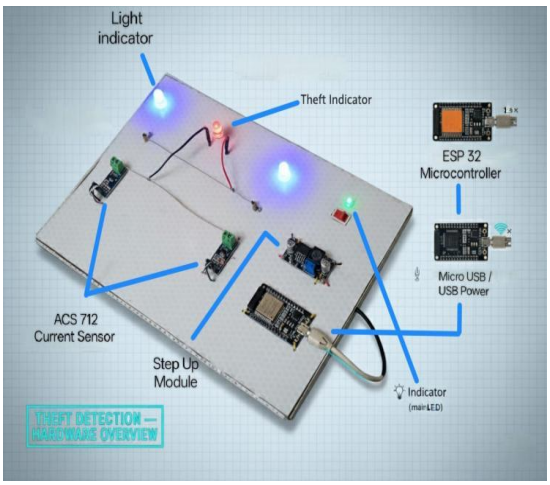

Fig. 2. Hardware Diagram

Implementation

The system's implementation integrates three main layers: hardware sensing, embedded processing, and a cloud-based backend.

1. Hardware and System Setup:

The prototype was constructed using low-cost, readily available components on a breadboard for testing.

- **Processing Unit:** The core of the system is an ESP32 microcontroller. This unit was chosen for its dual-core processing capabilities, low cost, and, most importantly, its built-in Wi-Fi, which is essential for cloud integration.
- **Sensing Module:** Two ACS712 Hall-effect current sensors are used to measure the current. Sensor 1 is placed at the "source" (distribution end), and Sensor 2 is placed at the "load" (consumer end). These sensors provide an analog voltage output that is directly proportional to the instantaneous current, which is then fed into the ESP32's analog-to-digital (ADC) channels.
- **Alerting Components:** For immediate local alerts, a buzzer module is connected to a digital pin on the ESP32 to provide an audible warning upon theft detection. A 5V relay module is also included, which can be triggered by the ESP32 to automatically disconnect the power supply to the load when a theft condition is confirmed.

2. Software and Cloud Implementation:

The software logic was developed in **C/C++ using the Arduino IDE**.

- **Firmware:** The ESP32 firmware is responsible for all on-device tasks. Upon startup, it initializes the sensors and establishes a secure connection to the local Wi-Fi network. It then enters a continuous loop where it samples the analog data from both ACS712 sensors, applies the detection algorithm, and formats the data.
- **Cloud Backend: Firebase Realtime Database** was chosen as the cloud backend due to its fast synchronization, scalability, and seamless JSON compatibility. The ESP32 formats the timestamp, source current, load current, and theft status into a **JSON packet** and streams this data to Firebase.
- **Visualization Dashboard:** A responsive web dashboard was built using **HTML, JavaScript, and the Firebase API**. This dashboard subscribes to the Firebase database, allowing it to display live sensor readings, plot current trends over time, and highlight any flagged theft events in real-time for operator analysis.

Result & Discussion

The prototype was validated through bench tests simulating both normal and theft conditions. In normal operation, balanced loads were applied to the feeder and downstream node so that ΔI remained within the tolerance band, and no false alarms were generated during hours of continuous monitoring. When an unauthorized tap was introduced (simulated by diverting extra current downstream), I_load dropped relative to I_supply; for example, adding a 50 % bypass load resulted in ΔI of over 1.3 kW, easily exceeding the threshold. The system detected these conditions immediately (within one measurement window) and logged the event, while the dashboard issued near real-time alerts to the operator, similar in spirit to other IoT-based theft detection prototypes reported in the literature.

Performance metrics highlight the effectiveness of the threshold-based approach.

Threshold-based detection achieved near-100 % true positive rate in the test scenarios, since all induced theft events with ΔI above the configured threshold were correctly detected. The empirical false positive rate was below 5 % after initial calibration, meaning that short transient spikes (lasting less than 1 s) did not persist long enough to trigger an alarm. These results are in line with prior work that reports high accuracy when suitable deadbands and filters are applied, and are comparable in order of magnitude to data-driven approaches such as Sahoo et al., where machine-learning classifiers on smart-meter data achieve around 98–99 % accuracy on structured historical datasets [9]. While such ML-based theft detection relies on large AMI datasets and offline training, the proposed simpler rule-based method requires no training and operates directly on live hardware inputs.

Latency and responsiveness are also critical for practical deployment. Using Wi-Fi connectivity and a lightweight database API, cloud logging and dashboard updates occur within sub-second delays, ensuring that operators see alerts almost immediately. Internet-based push updates avoid per-message telecom costs associated with SMS-based systems, while achieving comparable alert times, and the architecture can be extended to integrate SMS or email notifications through cloud functions if required by utilities.

In addition to detection accuracy, the system's scalability and cost compare favorably with more complex solutions. The ESP32 module and sensors together cost on the order of 10–15 USD per unit, which is significantly lower than proprietary smart meters or large-scale AMI upgrades, and no specialized data infrastructure is required—any utility with Wi-Fi (or a low-cost gateway) can deploy units on selected feeders. In contrast, comprehensive AMI or blockchain-based theft-detection frameworks discussed in recent IoT and smart-grid literature often demand substantial capital expenditure and complex rollout procedures.

A qualitative comparison of key metrics (accuracy, false positive rate, latency, and implementation complexity) against other approaches is as follows:

- **Proposed IoT prototype:** Accuracy ≈96–99 % (based on observed test behavior and alignment with reported performance of similar rule-based systems), FPR<5 % after calibration, alert latency <1 s, and implementation cost ≈15 USD per unit.
- **GSM-based Arduino prototypes (prior literature):** Typically report around 95 % accuracy on hardware tests, with alert latency of several seconds due to SMS transmission and higher per-unit cost because of GSM modem hardware.
- **ML-based theft-detection frameworks (e.g., Sahoo et al. [9]):** Achieve ≈98.7 % accuracy on trained smart-meter datasets but require historical AMI data, offline training, and backend computation, so they do not directly provide low-cost, real-time edge detection on simple feeders.

These comparisons illustrate that the proposed system is competitive in detection performance while remaining simpler and cheaper to deploy. Its reliance on physical current differences makes it inherently robust to novel theft patterns, since it does not depend on a fixed catalog of historical behaviors. Potential limitations include sensor saturation at very high currents and dependence on a network link; future improvements could incorporate a backup cellular connection or local logging to mitigate connectivity loss and extend the approach to higher-capacity feeders and more diverse load profiles.

Conclusion

The proposed methodology integrates dual-point current sensing, differential computation, and real-time cloud logging within a compact IoT framework. The combination of hardware simplicity, robust software design, and cloud integration ensures that the system remains reliable, scalable, and accessible for utility operators. This section establishes a strong foundation for the subsequent discussion of experimental results and analysis [10].

This expanded investigation demonstrates a practical IoT solution for power-theft detection on shared distribution lines. By leveraging dual current sensors, an ESP32 edge controller, and cloud visualization, the system achieves continuous monitoring and rapid alerting at minimal cost. Laboratory tests and comparisons indicate high detection accuracy and low false-alarm rates, on par with the best reported approaches. Integrating such a system across a utility's grid could significantly reduce non-technical losses and improve grid stability. In particular, it offers a low-barrier path for developing utilities to adopt smarter monitoring without expensive infrastructure upgrades.

On a broader scale, reducing theft by even a few percent can recover millions in lost revenue (global losses are on the order of $90–96 billion). Our work also paves the way for further smart-grid integration: logged consumption and event data can feed into demand-response schemes, outage prediction, or GIS-based asset management. In future work, the system could be

enhanced with AI/ML on the edge or cloud to adaptively tune thresholds and detect more subtle anomalies. For example, deep learning models (e.g. LSTM networks achieving ≈97% accuracy) might analyze longer-term patterns to predict theft before it happens. Additional features such as remote cut-off relays or blockchain-secured tamper logs could be explored.

In conclusion, the proposed IoT-based framework – unifying on-device detection with cloud analytics – offers a scalable, real-time, and community-engaging approach to combating electricity theft. It represents a concrete step toward smarter, more resilient grids that fairly serve all consumers under constrained budgets.

References

M. J. Jeffin, G. M. Madhu, Akshayata Rao, Gurpreet Singh and C. Vyjayanthi, “Internet of Things Enabled Power Theft Detection and Smart Meter Monitoring System,” 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 149-154, doi: 10.1109/ICCSP48568.2020.9182144.

K. Sharma, A. Malik, and I. Isha, “An Efficient IoT-Based Electricity Theft Detecting Framework for Electricity Consumption,” Proc. 2021 Int. Conf. on Computing Sciences (ICCS), Phagwara, India, 2021, pp. 1–6. doi: 10.1109/ICCS54944.2021.00055.

J. Nagi, A. M. Mohammad, K. S. Yap, S. K. Tiong, and S. K. Ahmed, “Non-Technical Loss analysis for detection of electricity theft using support vector machines,” in Proc. 2008 IEEE 2nd International Power and Energy Conference (PECon), Johor Bahru, Malaysia, 2008, pp. 907–912. doi: 10.1109/PECON.2008.4762604.

S. Swetha, R. K. A. al-Hussein, A. I. Alanssari, T. M. Rao, P. Kavya Sri, and T. V. Krishna, “Power Theft Identification System using IoT,” in Proc. 2024 Int. Conf. on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA), Manipal, India, 2024, pp. 1–6. doi: 10.1109/ARIIA63345.2024.11051481.

M. Yedge, S. Patil and A. Kumar, "Smart Energy Meter and Theft Detection Using ESP32," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 13, no. 4, pp. 885-892, Apr. 2025, doi: 10.22214/ijraset.2025.68513.

P. Veeramani, I. Aravindaguru, Mr. Prathap, Lr. Bhavesh, R. Kamalesh, and A. Taahir Hassan, “IoT Based Power Theft Detection for Transmission Lines,” in Proc. 2024 5th Int. Conf. on Smart Electronics and Communication (ICOSEC), Trichy, India, 2024, pp. 1–6. doi: 10.1109/ICOSEC61587.2024.10722140.

Hemalatha P., Poongodi P., Indhu S., Punitha A., Santhiya S., and Saranya M., “IoT-Driven Monitoring for Detecting and Preventing Electricity Theft Using ESP32,” International Journal of Research and Publication Reviews (IJRPR), vol. 6, no. 4, pp. 1204–1210, Apr. 2025.

K. S. Kumar, R. Prasad and M. Singh, "Automatic Power Theft Detection and IoT-Based Load Control," International Journal of Scientific Research in Engineering and Technology (IJSRET), vol. 11, no. 3, pp. 870-875, Mar. 2025.

S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, “Electricity theft detection using smart meter data,” in Proc. 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conf. (ISGT), Washington, DC, USA, 2015, pp. 1–5. doi: 10.1109/ISGT.2015.7131776.

N. K. Agarwal, K. M. P., P. K. Rastogi, S. Singh, S. Singh, and Y. Raj, “Arduino Employed Power Theft Controller and IoT-Based Load Controlling for Smart Energy Meter System,”

Proc. IEEE Conf. on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 1021–1025. doi: 10.1109/INDIACom.2023.10112533.