IoT-Based Transformer-to-Consumer Comparative Analysis for Real-Time Electricity Theft Detection

Hashir Qayum, Nabila Ayub, Gulzar Ahmad, Bilal Ur Rehman*
Department of Electrical Engineering, University of Engineering and Technology, Peshawar, Pakistan.
*Correspondence: bur@uetpeshawar.edu.pk

Citation | Qayum. H, Ayub. N, Ahmad. G, Rehman. B. U, "IoT-Based Transformer-to-Consumer Comparative Analysis for Real-Time Electricity Theft Detection" IJIST, Vol. 8 Issue. 6 pp 2498-2516, September 2026
DOI: https://doi.org/10.33411/IJIST/2021
Received | Aug 19, 2026 **Revised |** Aug 30, 2026 **Accepted |** Sep 06, 2026 **Published |** Sep 08, 2026.

Electricity theft is a significant source of non-technical losses in electrical distribution networks, particularly when unmetered loads or illegal connections occur between distribution transformers and registered consumers. This paper presents a low-cost IoT-based transformer-to-consumer comparative monitoring system for real-time screening of unexplained electricity losses. The proposed system uses ESP32 microcontrollers and PZEM-004T energy-monitoring modules to measure the output of a three-phase transformer and the consumption of individual single-phase consumers. Measurements are transmitted through Wi-Fi to a Supabase/PostgreSQL cloud backend at approximately five-second intervals, where aggregated registered-consumer power is compared with transformer output power. During the controlled proof-of-concept experiment, unaccounted power was approximately 0.13 kW under nominal operation. After introducing an additional unmetered load, the residual increased to 3.22 kW, exceeding the 0.5 kW experimental threshold. The PostgreSQL trigger consequently changed the theft status from false to true, and the dashboard displayed the alert during the next monitoring cycle. These results demonstrate the functional operation of the sensing, communication, cloud-processing, decision, and visualisation stages. However, structured measurement-error statistics, packet-delivery reliability, precise end-to-end response time, and statistical detection performance were not established during the present prototype experiment. Therefore, the generated alert should be interpreted as a potential theft or abnormal-loss inspection flag rather than conclusive evidence of electricity theft. Repeated calibration, communication-reliability testing, response-time analysis, and field-scale validation are recommended for future work.

Keywords: Electricity Theft; Non-Technical Losses; Internet of Things; ESP32; PZEM-004T; Transformer Monitoring; Comparative Analysis; Cloud Monitoring.

Introduction:

Electricity theft is a persistent non-technical loss (NTL) challenge in electrical distribution systems. Non-technical losses include unauthorized connections, meter tampering, meter bypassing, fraudulent reporting, and other forms of unmetered energy consumption. These losses negatively affect utility revenue, complicate demand management, increase the financial burden on legitimate consumers, and contribute to transformer overloading and reduced power system reliability. Early research on electricity theft detection primarily focused on statistical analysis and machine-learning-based identification of suspicious consumption patterns. At the same time, subsequent studies explored smart metering, transformer-level monitoring, deep learning, and hybrid detection approaches [1][2][3][4][5][6][7][8][9][10].

Recent studies indicate that electricity theft detection has evolved from conventional manual inspection and statistical techniques toward advanced approaches including supervised learning, deep learning, ensemble algorithms, anomaly detection, privacy-preserving analytics, and IoT-based monitoring frameworks [11][12][13][14][15]. Despite significant progress, existing approaches still face challenges related to class imbalance, limited availability of labelled theft datasets, model generalization, missing data, and measurement uncertainty [12][13][14][15][16]. Recent reviews have categorized electricity theft detection methods into data-driven, sequential analysis, neighborhood-based, and hardware-assisted approaches, highlighting the importance of practical IoT-based monitoring solutions for real-world deployment [15].

Although machine-learning-based approaches have demonstrated promising detection capabilities, many existing systems depend on extensive historical smart-meter datasets and require reliable communication infrastructure. In developing countries such as Pakistan, a major challenge remains the identification of the exact location of electricity losses within distribution networks. Feeder-level monitoring can indicate the presence of abnormal energy losses; however, it often cannot determine the specific street transformer or consumer group responsible for these losses.

To address this limitation, this research proposes an IoT-based transformer-to-consumer comparative monitoring framework that simultaneously measures transformer output power and registered consumer consumption. The system performs cloud-based comparative analysis to identify unexplained power differences and generate potential theft alerts. The proposed architecture integrates three-phase transformer monitoring, single-phase consumer monitoring, cloud data storage, automatic theft-status generation, GPS-based transformer identification, and a cost-effective scalable monitoring framework.

The primary contribution of this work is not the development of another high-accuracy classification model, but the establishment of a low-cost physical sensing and decision infrastructure capable of generating transformer-to-consumer residual data for immediate theft screening and future machine-learning-based analysis. The proposed system utilizes ESP32 microcontrollers, PZEM-004T energy monitoring modules, Wi-Fi communication, Supabase/PostgreSQL cloud infrastructure, and a web-based dashboard to provide real-time monitoring and visualization of distribution-level electricity consumption.

Problem Statement:

Electricity theft at the distribution level causes substantial non-technical losses and creates difficulties for utilities in identifying the precise location at which unaccounted electricity is being consumed. Conventional theft-detection practices largely depend on manual inspection, physical site visits, meter reading, and reporting by field personnel. Although feeder-level monitoring can indicate the overall magnitude of energy losses within a distribution area, it does not necessarily identify the street transformer or downstream consumer group responsible for the unexplained consumption. Consequently, locating illegal

connections can require considerable time and human effort. The problem addressed in this study is therefore the lack of a low-cost, real-time monitoring mechanism capable of extending loss identification from the feeder level to the street-transformer and registered-consumer levels while also providing automatic theft indication and geographic identification of the affected transformer.

Research Gap:

Existing electricity-theft detection approaches provide useful capabilities but leave an important practical gap between distribution-level monitoring and individual consumer-level identification. Conventional AMI and SCADA-based solutions may involve considerable deployment cost, while feeder-level systems generally provide insufficient spatial resolution to identify the transformer or household associated with abnormal losses. A particularly important gap is the limited availability of low-cost three-phase transformer-to-consumer comparative monitoring systems suitable for practical deployment in developing countries. Existing transformer-level initiatives may identify losses at a cluster level, but individual house-by-house assessment remains limited. Therefore, a need exists for a scalable architecture that simultaneously monitors three-phase transformer output and individual consumer consumption and automatically compares these measurements in real time to identify unexplained power discrepancies.

Novelty and Research Contribution:

The novelty of the proposed work lies primarily in the integration of transformer-level and consumer-level physical monitoring into a single low-cost IoT-based comparative architecture, rather than in claiming novelty for the individual sensing or communication components. The system combines three-phase monitoring at the distribution transformer with dedicated single-phase monitoring at registered consumer locations and performs the transformer-to-consumer comparison automatically in the cloud. This enables the system to move beyond feeder- or cluster-level loss identification toward finer localization of unexplained consumption.

A further contribution is the implementation of the theft-detection logic at the cloud database layer using automated database triggers. This allows the ESP32-based monitoring nodes to remain primarily responsible for sensing and data transmission, while comparative processing is performed centrally and can scale as additional nodes are registered. The research also demonstrates that three-phase transformer monitoring can be implemented using commercially available hardware and low-cost cloud infrastructure. In addition, the database and dashboard architecture were designed so that new transformer and consumer nodes can be incorporated without substantial changes to the detection or visualization logic.

The resulting contribution can therefore be summarized as a low-cost sensing-to-cloud architecture that integrates three-phase transformer monitoring, individual consumer monitoring, automated transformer-to-consumer comparative analysis, cloud-based theft-status generation, GPS-linked transformer localization, and real-time dashboard visualization within a scalable IoT framework.

Research Aim:

The aim of this research is to design and validate a low-cost and scalable IoT-based electricity theft monitoring system capable of performing near-real-time comparative analysis between the electrical power supplied by a three-phase distribution transformer and the power measured at its registered consumer nodes, while providing automatic cloud-based identification and geographic visualization of potential theft conditions.

Research Objectives:

The specific objectives of the proposed research are:

To design and test a three-phase transformer monitoring node capable of measuring voltage, current, active power, and frequency for each phase of a distribution transformer.

To design and test individual consumer monitoring nodes capable of measuring voltage, current, active power, and frequency for single-phase consumer loads.

To develop a cloud-based architecture that associates each monitored transformer with its registered consumer nodes and provides storage and near-real-time updating of transformer and consumer electrical measurements.

To implement automated cloud-based comparative analysis for identifying abnormal differences between transformer output power and aggregated registered-consumer power and for storing the corresponding potential-theft information.

To incorporate geographic identification of monitored transformers so that a transformer associated with a potential theft condition can be localized through the monitoring interface.

To develop a low-cost, low-latency, and scalable monitoring architecture using commercially available hardware and cloud infrastructure so that additional transformers and consumer nodes can be incorporated with minimal modification to the system.

Literature Survey:

Electricity theft detection has been widely investigated using statistical approaches, machine learning algorithms, smart metering infrastructure, and advanced data-driven techniques. Early studies mainly focused on identifying abnormal consumer behavior using historical consumption patterns. [1] introduced a support vector machine (SVM)-based customer preselection approach for detecting non-technical losses, demonstrating the potential of machine learning for identifying suspicious consumption profiles. [2][3] analyzed electricity theft mechanisms, their impacts on power utilities, and smart meter-based control strategies, while their subsequent work investigated SVM classification for automated theft detection. [4] further extended this concept by combining customer consumption patterns with distribution transformer information, highlighting the importance of hierarchical monitoring approaches for improving theft identification capability.

With the advancement of artificial intelligence, researchers have explored more sophisticated models for electricity theft detection. [5] reviewed artificial intelligence-based approaches and identified challenges related to model generalization, data quality, and practical deployment. [6] provided a comprehensive review of statistical and machine-learning techniques used for electricity theft detection in smart grid environments, emphasizing the importance of suitable features, reliable measurements, and effective classification methods. [7] investigated various non-technical loss detection methods and highlighted that network characteristics and measurement information significantly influence detection performance.

Several studies have focused on anomaly detection and deep learning approaches. [8] proposed an anomaly detection framework capable of distinguishing electricity theft from technical losses and defective meters, addressing one of the major challenges in practical deployment. [9] applied random matrix theory to analyze correlations within smart-grid consumption data for identifying abnormal patterns. [10] combined convolutional neural networks (CNNs) with random forest algorithms to extract consumption features and improve theft detection performance. [11] proposed a CNN-LSTM-based model that integrates spatial and sequential characteristics of electricity consumption data, demonstrating the capability of deep learning methods in capturing complex usage patterns.

Despite significant progress, recent studies indicate that no single detection approach provides universally optimal performance. [12] conducted a systematic review and concluded that detection accuracy strongly depends on dataset quality, feature selection, class imbalance, and evaluation methodology. [13][14] investigated deep learning techniques for non-technical loss classification, while evaluated decision-tree-based approaches for electricity theft detection. To overcome limitations associated with data imbalance and feature complexity, [16][17] proposed a hybrid AlexNet-AdaBoost-artificial bee colony model, while applied

AdaBoost ensemble learning for smart grid theft identification. [18] further explored feature synthesis and optimization techniques to improve detection performance.

Recent research has also focused on privacy preservation, representation learning, and hybrid intelligence techniques. [19] proposed a privacy-preserving electricity theft detection framework that protects both customer data and model information. [20] applied contrastive learning to improve the representation of normal and fraudulent consumption patterns. [21] developed a hybrid deep-learning framework combining optimization techniques, convolutional feature extraction, cost-sensitive learning, and recurrent modelling. Similarly, [22][23] evaluated ensemble machine-learning methods for smart-meter-based theft detection, while introduced an MLP-GRU-based framework with data balancing strategies. More recent studies have investigated robust resampling techniques, stacked learning models, CNN-AdaBoost approaches, and Pakistan-focused machine-learning solutions for electricity theft detection [24][25][26]. Table 1 summarizes representative electricity theft detection approaches, their main contributions, and limitations identified from previous studies.

Table 1. Representative literature and relevance

Ref.	Method	Main contribution	Limitation / relevance
[1][3]	SVM / smart metering	Early automated customer screening	Historical data dependent
[4]	Consumption + transformer	Hierarchical detection	Requires downstream data
[7][9]	Anomaly / mathematical	Considers network behavior	Higher analytical complexity
[10][11]	CNN / CNN-LSTM	Learns temporal features	Needs training data
[12]	Systematic review	Compares NTL methods	No deployment architecture
[16][18]	Hybrid / ensemble	Addresses imbalance and features	Model complexity
[19][21]	Privacy / contrastive / hybrid DL	Security and representation learning	Computational/data requirements
[22][26]	Ensemble / ML / hybrid	Improved classification	Mostly smart-meter data driven
[27][28]	Recent reviews	Dataset and IoT perspectives	Motivate complementary hardware layer

Although machine-learning and deep-learning methods have achieved promising results, their practical implementation often depends on large historical smart-meter datasets, accurately labeled theft cases, and reliable communication infrastructure. These requirements create challenges in developing regions where widespread smart metering is limited. Recent reviews have emphasized that dataset availability, measurement uncertainty, and deployment constraints remain major challenges in real-world electricity theft detection systems [27][28].

Therefore, a complementary hardware-based monitoring approach is required to provide reliable physical measurements before applying advanced analytics. The proposed system addresses this gap by establishing a transformer-to-consumer measurement layer that directly compares supplied and consumed power. Unlike purely data-driven approaches, this framework provides real-time residual power information, enabling immediate theft screening while generating valuable time-series data for future adaptive anomaly detection and machine-learning models.

Proposed System Design and Implementation:

Overall System Architecture:

The proposed IoT-based electricity theft detection and monitoring system is organized into four integrated functional layers: transformer-side sensing, consumer-side sensing, cloud-based processing and storage, and web-based visualization. The transformer node is installed at the distribution side and monitors all three phases, whereas one or more consumer nodes monitor the electricity consumption of individual single-phase loads. The measurements from both node types are transmitted to a Supabase PostgreSQL cloud backend, where the data are stored and the comparative theft-detection mechanism is executed automatically.

A deliberate separation of responsibilities was adopted in the implementation. The embedded nodes acquire electrical parameters and upload JSON-formatted measurements; the cloud backend stores the measurements and executes the theft-detection logic; and the web dashboard retrieves the processed data for monitoring and visualization. This modular arrangement reduces the computational burden on the sensing nodes and makes the architecture easier to maintain and extend. The complete sensing-to-visualization flow is illustrated in Figure 1.

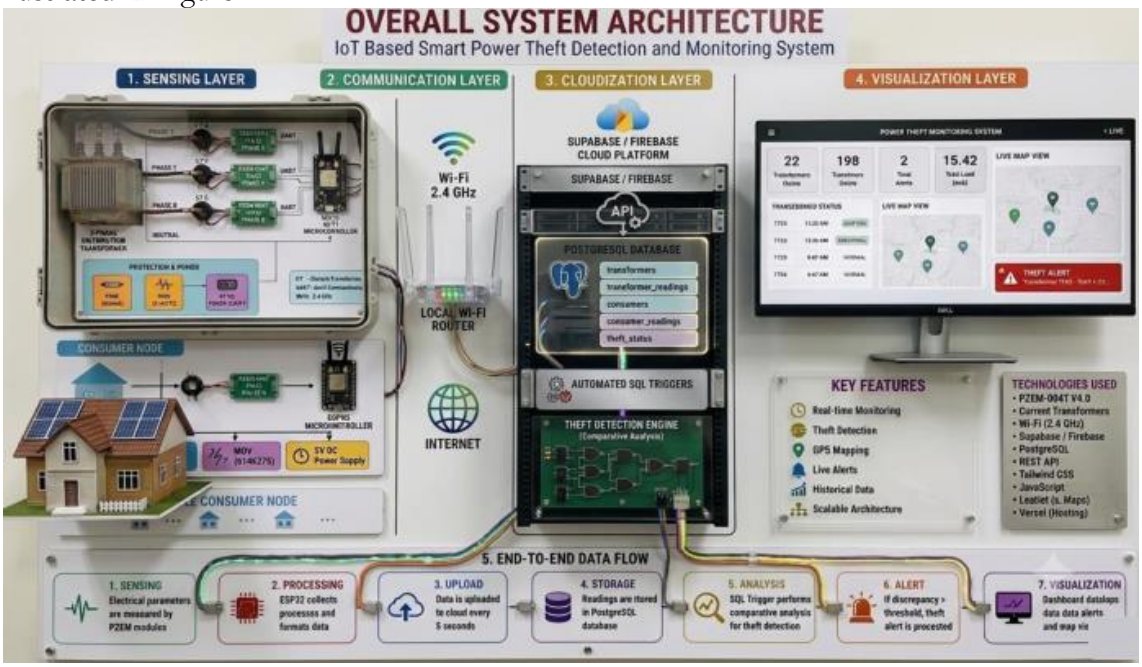

Figure 1. Overall system architecture of the IoT-based power theft detection and monitoring system.

Transformer Monitoring Node:

The transformer monitoring node is the more complex of the two embedded node types because a three-phase distribution transformer requires three independent measurement channels. Three PZEM-004T V4.0 energy-monitoring modules are used, one for each phase, and all three are connected to a single ESP32 microcontroller. The ESP32 polls the modules sequentially using Modbus RTU communication over UART. This work based on the implementation uses dynamic UART2 pin remapping to switch among the three phase-specific communication paths during each polling cycle.

MES-62/40 current transformers are used on the transformer side to measure phase current while maintaining separation between the distribution conductors and the low-voltage measurement circuitry. The transformer node acquires voltage, current, active power, and frequency for the three phases. The measured data are then transmitted to the cloud approximately every five seconds through Wi-Fi using HTTP POST requests. Figure 2 shows the transformer node arrangement.

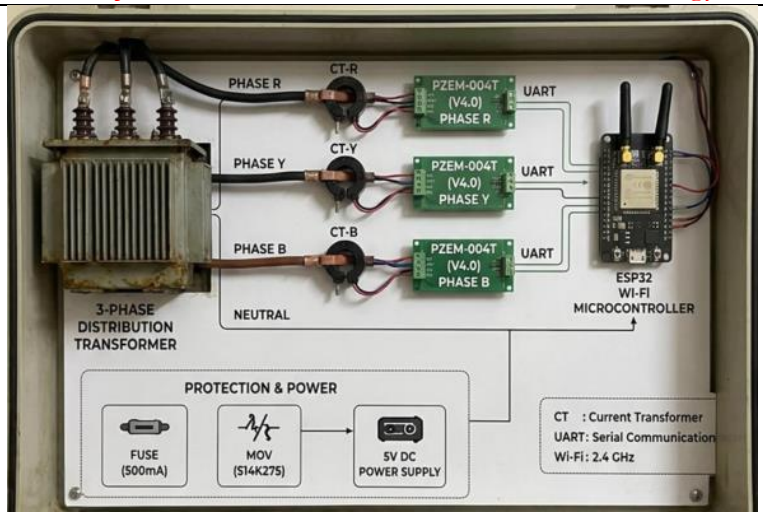

Figure 2. Transformer monitoring node architecture.

Consumer Monitoring Node:

The consumer monitoring node is intentionally simpler than the transformer node because the targeted residential consumers operate on a single-phase supply. Each consumer node therefore uses one PZEM-004T V4.0 energy-monitoring module connected to an ESP32 microcontroller. The module uses its built-in current transformer, rated up to 100 A, so a separate external current transformer is not required at the consumer side.

Because only one PZEM module is connected to the ESP32, fixed UART2 pins are sufficient and no dynamic UART remapping is required. Each consumer node continuously measures the electrical parameters of the connected load and uploads the measurements to the cloud. The node is associated with its supplying transformer in the database, allowing the backend to aggregate registered consumer consumption for transformer-to-consumer comparison. The consumer-node implementation is shown in Figure 3.

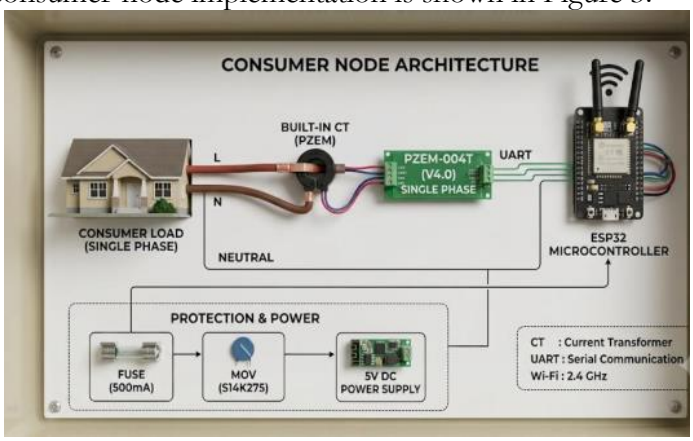

Figure 3. Consumer monitoring node architecture.

Wi-Fi Communication Flow:

Both transformer and consumer nodes use the integrated Wi-Fi capability of the ESP32 to transmit measurements to the Supabase cloud server. The PZEM-004T modules provide the electrical measurements to the ESP32, which processes the values and converts them into JSON payloads. These payloads contain node identification and electrical measurements such as voltage, current, active power, and frequency, together with the relevant timing information.

The nodes connect to a local 2.4 GHz Wi-Fi router, which provides Internet access to the Supabase REST API endpoint. Measurements are uploaded approximately every five seconds. Wi-Fi was selected for the prototype primarily to avoid recurring GSM airtime costs

during testing. The work also identifies the corresponding limitation: the system depends on Wi-Fi availability and would require another communication option for remote deployment. The communication path is summarized in Figure 4.

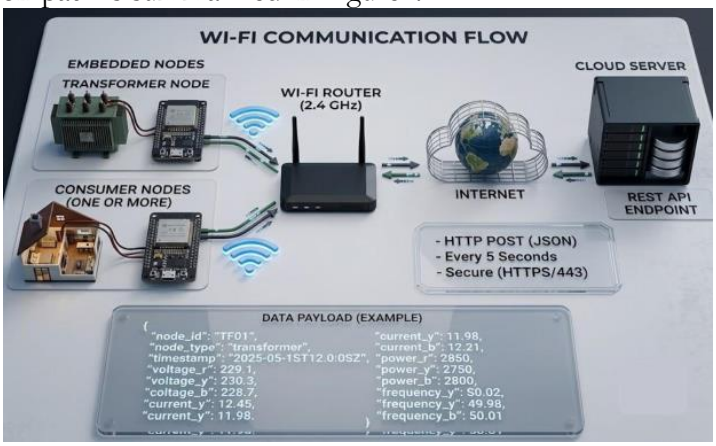

Figure 4. Wi-Fi communication flow between the embedded monitoring nodes and the cloud backend.

Cloud Backend Architecture:

Supabase was selected as the backend platform because it provides a managed PostgreSQL database and REST API functionality suitable for the prototype upload rate. The database stores transformer information, consumer information, transformer telemetry, consumer telemetry, and theft-status information. Transformer records include identifiers, geographic coordinates, and theft thresholds, while consumer records are linked to their associated transformer using database relationships.

The main feature of the backend is automatic theft analysis using PostgreSQL triggers. When a new transformer reading is inserted, a trigger starts the comparative detection process. The backend also removes older telemetry records to remain within the storage limits of the free-tier configuration used in the prototype. Figure 5 presents the backend structure, including data ingestion, database tables, the automated trigger, theft-detection logic, and data-retention process.

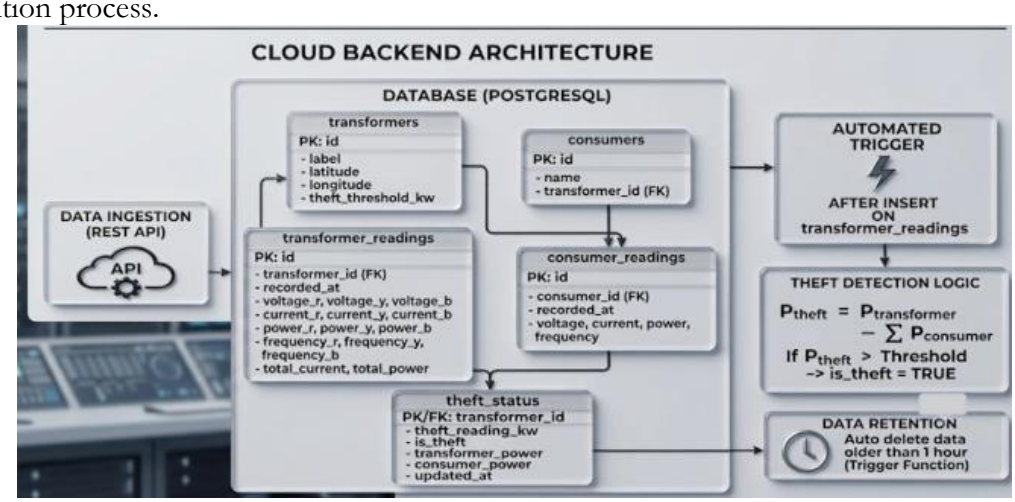

Figure 5. Supabase /PostgreSQL cloud backend and automated theft-detection architecture.

Comparative Theft-Detection Mechanism:

The theft-detection mechanism is based on a direct comparison between the active power measured at the transformer and the combined active power reported by the registered consumer nodes connected to that transformer. The backend first obtains the transformer output power and the consumer measurements, sums the consumer power values, and then calculates the unaccounted power difference as:

$$P_{unaccounted} = P_{transformer} - \Sigma P_{consumer,i}$$

In this expression, P_unaccounted is the power difference, P_transformer is the active power measured at the transformer output, and ΣP_consumer,i is the sum of active power measured by all registered consumer nodes associated with the transformer. The research describes this relation as the Comparative Analysis Equation. If the calculated difference exceeds the configured theft threshold, the backend updates the theft-status table and marks the transformer as being under a potential theft condition.

In a practical distribution network, the calculated residual should not be interpreted as unauthorized consumption alone. It can be expressed conceptually as:

$$P_{unaccounted} = P_{unauthorized} + P_{transformer\ loss} + P_{feeder\ loss} + P_{unmonitored\ legitimate\ load} + \varepsilon_{sensor} + \varepsilon_{time}.$$

Transformer core and copper losses, feeder (I^2R) losses, PZEM and current-transformer errors, phase imbalance, and differences between transformer and consumer measurement times can therefore contribute to the residual. Consequently, a persistent residual exceeding the configured threshold is treated as an indicator of potential theft or abnormal loss that requires field investigation, rather than as direct proof of illegal electricity consumption.

For prototype validation, the 0.5 kW threshold was selected as an engineering decision level between the observed normal residual of 0.13 kW and the simulated-theft residual of 3.22 kW. It provides a margin of 0.37 kW above the observed baseline. A basic sensitivity assessment showed that thresholds of 0.25, 0.5, 1.0, and 2.0 kW produced the same classification for the two observed conditions. However, because the study involved limited controlled observations, the selected threshold should be regarded as a preliminary inspection trigger rather than a statistically optimized or universal theft-detection threshold. Future field studies should determine the threshold using repeated measurements, sensor uncertainty, technical losses, and normal residual variability.

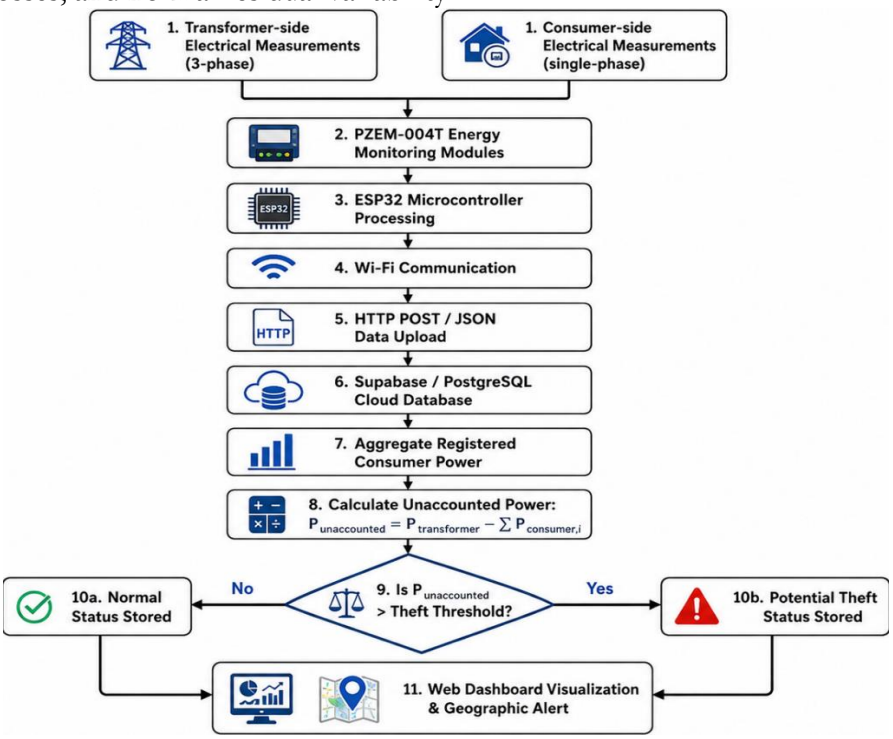

Figure 6. Operational flow of the proposed IoT-based transformer-to-consumer electricity theft detection system.

The operational sequence of the proposed electricity theft detection system is illustrated in Figure 6. Electrical parameters are initially measured at both the three-phase distribution transformer and the registered single-phase consumer nodes using PZEM-004T

energy-monitoring modules. The measured values are acquired and processed by ESP32 microcontrollers and subsequently transmitted through Wi-Fi to the Supabase/PostgreSQL cloud backend using HTTP POST requests with JSON-formatted payloads. After receiving the measurements, the cloud backend associates consumer readings with their corresponding transformer and calculates the total registered consumer power. The unaccounted power is then determined by subtracting the aggregated consumer power from the measured transformer output power. This residual value is compared with the predefined theft-detection threshold through an automated PostgreSQL trigger. If the calculated residual exceeds the configured threshold, the system updates the theft status and identifies the corresponding transformer as a potential theft location; otherwise, the system retains the normal operating status. The resulting information is stored in the cloud database and subsequently retrieved by the web-based dashboard for real-time visualization and geographic identification of the affected transformer.

Web-Based Dashboard Visualization:

A web-based dashboard was developed to provide real-time visualization of transformer and consumer telemetry. The interface displays voltage, current, active power, and frequency values, together with the calculated discrepancy and theft status. Data are fetched from the Supabase tables and updated continuously as new measurements are received.

The dashboard also incorporates transformer location information using OpenStreetMap. When a transformer is flagged, the interface visually highlights the affected transformer and provides a map view to support location-based investigation. The dashboard was deployed using Vercel. Figures 7(a) and 7(b) show the detailed alert view and the geographic overview.

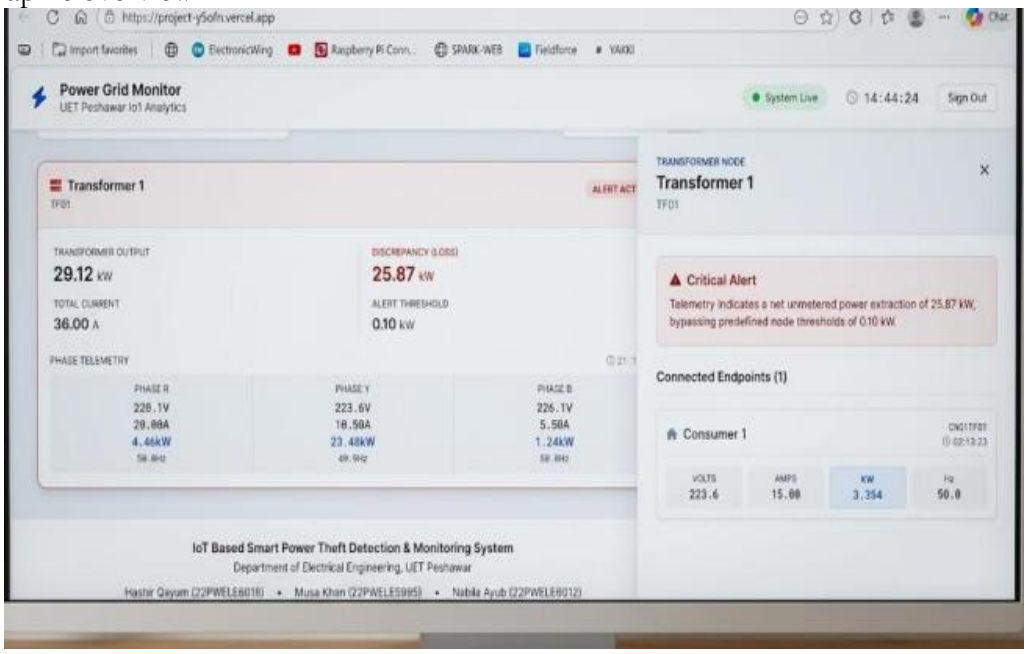

Figure 7(a). Detailed dashboard view showing transformer telemetry, discrepancy, connected consumer information, and critical alert.

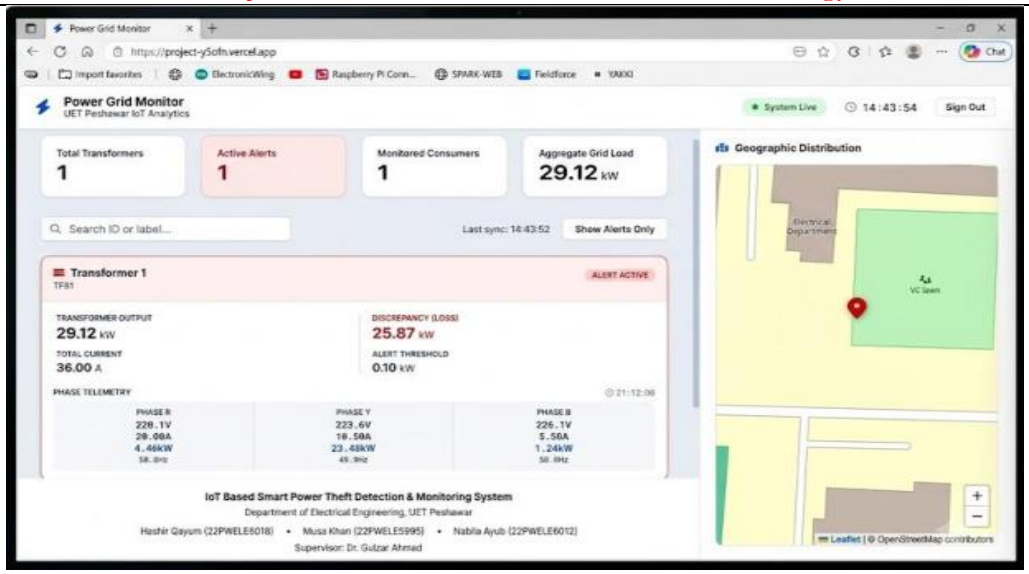

Figure 7(b). Dashboard overview showing active alerts, transformer status, aggregate load, and geographic location.

Results and Testing:

Hardware Verification:

The hardware was verified component by component before complete system integration. The PZEM-004T modules were tested first because inaccurate sensor measurements would directly affect the transformer-to-consumer power comparison. After the PZEM modules were verified, the ESP32 boards and current transformers were tested before the complete monitoring nodes were assembled.

Verification of PZEM-004T V4.0 Energy-Monitoring Modules:

The PZEM-004T modules were connected to a computer through a USB/UART interface and Modbus communication was implemented to monitor voltage, current, active power, energy, power factor, and frequency in real time. The modules were connected to a known AC load and their measurements were compared with multimeter readings. During this verification, stored values present in the modules were cleared using the Modbus reset command 0x42. A byte-order/parsing issue was also identified: the initial interpretation produced current and power values approximately ten times greater than their actual values. The parsing logic was corrected before the modules were integrated into the final firmware. The PZEM-004T modules and external MES current transformers were subjected to functional verification rather than formal metrological calibration. The PZEM-004T readings were compared with available multimeter measurements to confirm reasonable measurement behaviour and identify major implementation errors. This process revealed a byte-order and parsing problem that initially produced current and power readings approximately ten times greater than the expected values. The parsing logic was corrected before the modules were incorporated into the final monitoring system.

ESP32 DevKit V1 Testing:

The ESP32 boards were tested before soldering and final hardware integration. Firmware uploading through the Arduino IDE and USB connectivity were verified. GPIO pins 4, 5, 16, 17, 18, and 19 were tested using a digital-output program, and normal output behavior was observed. With the PZEM modules attached, the 3.3 V rail was measured at 3.284 V. Wi-Fi connectivity was also checked, and the boards successfully obtained network addresses.

UART loopback testing was performed before connecting the measurement modules. Repeated operating cycles showed stable serial communication without observed resets or

communication drops. One ESP32 initially contained an old core dump that interfered with booting; the stored data were erased before further testing.

Current Transformer Verification:

Two current-transformer arrangements were used. At the consumer side, the PZEM-004T built-in ring-core current transformer was used for measurements up to 100 A. At the transformer node, three external MES current transformers rated at 400/5 A were used. The transformer-side arrangement was checked using a test load, and the measured values were compared with a clamp meter. A current scaling factor was incorporated into the firmware to align the PZEM measurement with the external current-transformer configuration.

Similarly, the transformer-side MES current-transformer arrangement was compared with a clamp meter, and a current-scaling factor was incorporated into the firmware. However, a structured calibration dataset containing repeated measurements at multiple load points was not recorded. Therefore, quantitative measurement errors, percentage deviations, confidence intervals, and uncertainty values cannot be reported for the present prototype. The electrical measurements should consequently be interpreted as supporting functional proof-of-concept validation rather than traceable metrological characterization. Future work should calibrate each measurement channel against a reference power analyzer over multiple resistive and inductive load levels and report mean error, maximum percentage error, standard deviation, RMSE, and expanded measurement uncertainty.

Communication Testing:

Modbus RTU Communication Verification:

Modbus RTU communication was verified by observing the serial output in the Arduino IDE while the firmware was operating. Requests and responses were observed for each polling cycle, and the returned values were printed for inspection. In the transformer node, three PZEM modules were polled during each loop, one for each phase. An address-related issue was encountered because two PZEM modules retained the default address 0xF8. The firmware was therefore configured to use 0xF8 for each module while communicating through separate pin paths. Because the PZEM modules did not share the same physical bus, this arrangement avoided communication collisions in the implemented prototype.

Supabase Cloud Communication Verification:

Cloud communication was tested by operating the transformer and consumer nodes simultaneously while observing the Supabase table editor. New rows appeared in the transformer_readings and consumer_readings tables approximately every five seconds. The transformer and consumer identifiers were correctly associated with their configuration records through the database relationships, and the theft_status table updated automatically.

When the transformer node remained active while the consumer contribution was removed, the calculated unaccounted power increased because the transformer continued to report a load while the consumer contribution fell to zero. The is_theft Boolean changed to true within one polling cycle. The communication parameters used in the prototype are summarized in Table 2.

Table 2. Cloud communication parameters used during prototype testing.

Parameter	Implemented value
Communication method	HTTP POST
Payload format	JSON
Nominal upload interval	Approximately 5 s

Theft-Detection Verification:

Simulated Theft Scenario:

The complete theft-detection chain was evaluated in a controlled environment. While the system was operating normally, an additional load was connected directly to the main power line so that the load was measured at the transformer side but bypassed the consumer

node. This reproduced the measurement effect of an unmetered load connected between the transformer measurement point and the registered consumer measurement point.

The additional load increased the difference between transformer-side power and registered consumer-side power. The measurements were uploaded to the cloud, where the comparative algorithm processed the discrepancy and updated the theft status.

Threshold Trigger Response:

A PostgreSQL trigger in Supabase executed the detection logic automatically whenever a new transformer reading was inserted. The latest transformer power was compared with the corresponding consumer power and the resulting difference was evaluated against the experimental threshold of 0.5 kW. Because the additional load produced a discrepancy greater than the threshold, the database changed the is_theft status to true and recorded the missing-power value in the theft_reading_kw field without manual intervention.

Dashboard Alert Behavior:

The dashboard detected the updated theft status on the next five-second polling cycle. The affected transformer card changed to a red-highlighted alert state, the status badge indicated an alert, and the transformer map marker changed from blue to red. The consumer detail panel displayed a critical alert containing the measured discrepancy. When the unmetered load was removed, the next polling cycle returned is_theft to false and the dashboard returned to the normal state.

System Limitations Observed:

Wi-Fi Dependency:

The endpoint architecture depends on a 2.4 GHz Wi-Fi connection. If the local router or Internet connection fails, telemetry upload stops until the connection is restored. The embedded logic automatically reconnects and resumes streaming once network connectivity becomes available again. In the present implementation, this dependence limits deployment in locations where reliable Wi-Fi is not available.

Free-Tier Data-Retention Window:

The prototype uses the free tier of Supabase/PostgreSQL. With a five-second polling interval, each node can generate thousands of records per day, making long-term raw-data retention impractical under the available free-tier storage. The implemented configuration therefore focuses on real-time and short-term analysis and automatically removes telemetry records older than approximately one hour.

Supabase Tables and Data Structure:

The database structure was verified using representative records from the transformer, consumer, consumer_readings, and theft_status tables. The transformer table stores identification, geographic position, and threshold information, whereas the consumer table maps each consumer node to its supplying transformer.Table 3 represents the transformer configuration and Table 4 represents the consumer to transformer mapping.

Table 3. Representative transformer configuration records.

ID	Label	Latitude	Longitude	Theft threshold (kW)
TF01	DEE UET TFO	34.002347	71.4852	1.5
TF02	Sample	34.018	71.5300	1.0

Table 4. Representative consumer-to-transformer mapping.

Consumer ID	Name	Transformer ID
CN01TF01	EE Dept Main Laboratory Block	TF01
CN01TF02	Workshop Node Complex	TF02

The consumer_readings table stores timestamped single-phase electrical measurements. Representative records are reproduced in Table 5 and Table 6 represents the most important validation records contained in the theft_status table.

Table 5. Representative consumer_readings records reproduced.

ID	Consumer ID	Recorded at	Voltage (V)	Current (A)	Power (W)	Frequency (Hz)
5001	CN01TF01	2026-06-02 10:00:00+05	223.1	18.2	4060.4	50.0
5002	CN02TF01	2026-06-02 10:00:00+05	222.8	18.2	4344.6	50.0
5003	CN01TF01	2026-06-02 10:05:00+05	222.4	18.2	4069.9	50.0
5004	CN02TF01	2026-06-02 10:05:00+05	221.9	18.2	4304.8	50.0

Table 6. Theft-status records for nominal and simulated-theft conditions.

Parameter	**Nominal state**	**Theft state**
Transformer ID	TF01	TF01
Unaccounted power (W)	129.5	3220.9
Unaccounted power (kW)	0.13	3.22
is_theft	False	True
Transformer power (W)	8534.5	11595.6
Consumer power (W)	8405.0	8374.7
Updated at	2026-06-02 10:00:02+05	2026-06-02 10:05:01+05
Parameter	Nominal state	Theft state
Transformer ID	TF01	TF01

Experimental Result:

Under the nominal condition, the transformer power was 8534.5 W and the registered consumer power was 8405.0 W, giving an unaccounted power of 129.5 W, or approximately 0.13 kW. This value remained below the 0.5 kW threshold used in the controlled experiment and the theft flag remained false.

During the simulated-theft condition, the transformer power increased to 11595.6 W while registered consumer power was 8374.7 W. The resulting unaccounted power was 3220.9 W, or approximately 3.22 kW. Because this value exceeded the 0.5 kW threshold, the PostgreSQL trigger set the theft flag to true. The dashboard subsequently displayed the alert during the next polling cycle. These results verify the operation of the prototype sensing, communication, cloud-processing, and visualization chain for the controlled test.

The present experiment validates the functional operation of the proposed system rather than its statistical performance. Because repeated independent trials and synchronized reference measurements were not collected, the mean, standard deviation, measurement error, detection latency, and experimental variability could not be reliably estimated. Therefore, the residual values of 0.13 kW and 3.22 kW should be interpreted as representative observations from the normal and simulated-theft conditions, respectively. Future validation should include repeated normal and theft experiments, calibrated reference instruments, and synchronized timestamps to determine measurement accuracy, detection latency, variability, and confidence intervals.

Discussion:

The experimental results demonstrate the successful operation of the complete sensing-to-decision chain of the proposed IoT-based electricity theft monitoring system. The implemented prototype integrates electrical parameter measurement, ESP32-based embedded processing, Modbus RTU communication, Wi-Fi data transmission, cloud storage, automatic transformer-to-consumer comparison, database-trigger-based decision making, and web-based visualization. Unlike many electricity theft detection studies that primarily evaluate

classification algorithms using historical smart-meter datasets, the present work demonstrates a physical monitoring architecture capable of generating real-time transformer-to-consumer power-balance information. This makes the proposed system particularly relevant as an infrastructure layer for immediate abnormal-loss screening as well as for the future development of data-driven detection models.

The most significant result obtained during the controlled experiment was the increase in unaccounted power from approximately 0.13 kW under nominal operating conditions to 3.22 kW after the introduction of an unmetered load. The 3.22 kW residual exceeded the 0.5 kW threshold used specifically for the controlled theft-detection experiment, causing the database trigger to change the theft status from false to true. The dashboard subsequently displayed the corresponding alert during the next monitoring cycle. This result confirms that the implemented architecture can detect a sufficiently large transformer-to-consumer power discrepancy under the tested conditions.

However, the experimental result should not be interpreted as evidence of 100% electricity-theft detection accuracy. The validation consisted of a controlled simulated-theft event rather than a large-scale field study containing numerous normal and theft cases under varying load, environmental, communication, and network conditions. Consequently, statistical performance indicators such as accuracy, sensitivity, specificity, precision, recall, false-positive rate, and false-negative rate cannot be determined from the present experiment. A larger field dataset containing both confirmed normal and confirmed abnormal operating conditions would be required before such performance measures could be reported reliably.

Another important consideration is that the calculated unaccounted power should not be treated as direct proof of electricity theft. In practical distribution networks, the difference between transformer output power and aggregated registered consumer power may contain several contributions in addition to unauthorized consumption. These can include transformer copper and core losses, feeder losses, current-transformer scaling errors, PZEM measurement uncertainty, phase imbalance, timing differences between transformer and consumer measurements, and legitimate loads that are not represented by registered consumer nodes. Therefore, the output of the present system is more appropriately interpreted as an abnormal-loss or potential-theft flag that identifies a transformer requiring further investigation rather than as a final determination of illegal activity.

The use of a fixed threshold is suitable for proof-of-concept validation because it provides a transparent and computationally simple decision mechanism. Nevertheless, a single fixed threshold may not remain appropriate across transformers of different ratings, loading levels, feeder lengths, technical-loss characteristics, and numbers of connected consumers. In this work, a partial current-transformer bypass producing a relatively small deviation of approximately 0.3 kW is discussed as an example of an abnormal condition that might remain below a 0.5 kW threshold. This illustrates the limitation of purely threshold-based detection and motivates the use of adaptive or transformer-specific decision limits in future implementations.

For practical deployment, the threshold could be dynamically selected according to transformer loading, expected technical losses, sensor accuracy, and historical residual behavior. A persistence criterion could also be introduced so that an alert is generated only when an abnormal residual remains present for several consecutive measurement intervals. Such an approach would reduce the likelihood of transient variations being interpreted as theft. Timestamp synchronization between transformer and consumer nodes would further improve the validity of the comparison by ensuring that measurements representing approximately the same operating instant are evaluated together.

Communication and data storage also represent important limitations of the current prototype. Measurements are transmitted approximately every five seconds, providing near-

real-time monitoring but simultaneously generating a large volume of telemetry. Under the free-tier Supabase configuration used in the prototype, long-term retention of all raw measurements is impractical, and the implemented system therefore focuses primarily on short-term and real-time monitoring. Similarly, the present architecture depends on 2.4 GHz Wi-Fi connectivity. Loss of router or Internet connectivity interrupts cloud telemetry until the embedded node reconnects. A field-ready implementation should therefore incorporate local data buffering so that measurements generated during communication outages can be temporarily stored and transmitted after connectivity is restored.

Cellular communication represents another possible improvement for transformers installed in locations where Wi-Fi is unavailable. Technologies such as GSM/LTE-based communication could extend deployment coverage, while local SD-card storage could provide offline buffering and longer-term measurement retention. A production implementation would additionally require stronger cybersecurity provisions, including protected device credentials, authenticated communication, encrypted data transfer, role-based access to the monitoring dashboard, secure database policies, and continuous monitoring of communication health.

The present architecture should therefore be considered complementary to machine-learning-based electricity theft detection rather than a replacement for it. The physical transformer-to-consumer measurement layer provides interpretable residual power information, while long-term operation of the proposed nodes could generate the time-series datasets needed to train transformer-specific statistical or machine-learning models. Such models could learn normal variations in transformer losses and consumption patterns and potentially distinguish persistent suspicious deviations from legitimate technical losses. This direction is consistent with recent research emphasizing adaptive, ensemble, deep-learning, and data-driven electricity theft detection techniques [15][23][24][25][26][27][28].

A hybrid architecture combining physical power-balance monitoring with data-driven anomaly detection may therefore provide a stronger long-term solution. The physical comparison maintains transparency and provides direct information about unexplained power flow, while machine-learning algorithms could improve sensitivity to smaller or more complex theft patterns that may not exceed a predefined threshold.

Practical Implications:

The proposed system has practical potential as a low-cost early-warning and inspection-support tool for electricity distribution utilities. By simultaneously monitoring three-phase transformer output and registered consumer consumption, the system can automatically identify unexplained power discrepancies and associate them with a particular distribution transformer. The integration of cloud-based processing, automatic theft-status generation, and GPS-linked dashboard visualization can help utility personnel narrow the location of abnormal losses before conducting physical inspection, thereby reducing the time and manpower required for conventional transformer-by-transformer or consumer-by-consumer checking. Because the prototype is based on commercially available ESP32 microcontrollers, PZEM-004T modules, and cloud infrastructure, the architecture also provides a relatively accessible pathway for extending monitoring from feeder- or cluster-level assessment toward street-transformer and consumer-level analysis. With improvements in communication reliability, data storage, measurement synchronization, and adaptive detection, the system could support more efficient loss monitoring and targeted field investigation in practical distribution networks.

Limitations:

The proposed system is subject to several limitations that should be considered when interpreting the experimental results. The current prototype depends on a 2.4 GHz Wi-Fi connection, meaning that telemetry transmission is interrupted whenever Internet connectivity

is unavailable. In addition, the five-second sampling interval produces a large volume of data, while the free-tier Supabase configuration provides only limited storage for long-term historical records. The comparative detection method also relies on a fixed threshold, which may not be suitable for transformers operating under different loading and network conditions. Furthermore, the calculated unaccounted power may be affected by transformer and feeder losses, current-transformer scaling errors, PZEM measurement uncertainty, phase imbalance, timing differences between transformer and consumer measurements, and legitimate loads not represented by registered consumer nodes. Therefore, the generated theft status should be interpreted as a potential-theft or abnormal-loss indication rather than conclusive evidence of illegal electricity consumption. Finally, the conducted results are based on a controlled prototype experiment rather than a large-scale field deployment, and consequently statistical measures of detection accuracy, false-positive rate, and false-negative rate cannot yet be established.

An additional limitation is that the PZEM-004T modules and external current transformers were functionally verified but were not subjected to formal traceable calibration. Sensor uncertainty and current-transformer scaling error may therefore contribute to the calculated transformer-to-consumer residual, and quantitative accuracy claims cannot be established from the present experiment.

Although the prototype was developed using commonly available components, its complete lifecycle cost was not formally evaluated. Installation, communication, cloud-service, calibration, and maintenance costs may vary according to location and deployment scale. Therefore, no quantitative cost advantage over conventional monitoring systems is claimed. Future work should provide a detailed bill of materials and lifecycle cost comparison based on supplier quotations and field-deployment data.

Conclusion:

This study developed and validated a low-cost IoT-based transformer-to-consumer monitoring system for real-time identification of unexplained electricity losses. The proposed architecture integrates three-phase transformer monitoring, single-phase consumer monitoring, ESP32 controllers, PZEM-004T modules, Modbus RTU communication, Wi-Fi connectivity, a Supabase/PostgreSQL cloud backend, and a web-based dashboard. Experimental testing confirmed reliable sensing, communication, cloud-based comparative analysis, and automatic theft-status generation. During the controlled theft simulation, unaccounted power increased from approximately 0.13 kW to 3.22 kW, exceeding the 0.5 kW experimental threshold and triggering an alert. These results demonstrate the functional feasibility of the proposed system as a low-cost abnormal-loss screening and monitoring solution. However, the findings represent proof-of-concept validation rather than field-scale detection accuracy, and the generated theft indication should be treated as an inspection flag because technical losses, measurement uncertainty, synchronization errors, and unregistered legitimate loads may also contribute to the calculated power discrepancy. Future work should focus on adaptive detection thresholds, cellular backup communication, local data buffering, synchronized measurements, stronger cybersecurity, and long-term cloud storage. Extended field validation involving multiple consumers and operating conditions is also recommended. The collected data may subsequently support machine-learning-based anomaly detection and reduce false alarms.

References:

[1] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, "Nontechnical loss detection for metered customers in power utility using support vector machines," *IEEE Trans. Power Deliv.*, vol. 25, no. 2, pp. 1162–1171, Apr. 2010, doi: 10.1109/TPWRD.2009.2030890.

[2] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview,

issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, Feb. 2011, doi: 10.1016/J.ENPOL.2010.11.037.

[3] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," *2011 IEEE/PES Power Syst. Conf. Expo. PSCE 2011*, 2011, doi: 10.1109/PSCE.2011.5772466.

[4] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016, doi: 10.1109/TSG.2015.2425222.

[5] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The Challenge of Non-Technical Loss Detection using Artificial Intelligence: A Survey," *Int. J. Comput. Intell. Syst.*, vol. 10, no. 1, pp. 760–775, Jul. 2017, doi: 10.2991/ijcis.2017.10.1.51.

[6] T. Ahmad, H. Chen, J. Wang, and Y. Guo, "Review of various modeling techniques for the detection of electricity theft in smart grid environment," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 2916–2933, Feb. 2018, doi: 10.1016/J.RSER.2017.10.040.

[7] G. M. Messinis and N. D. Hatziargyriou, "Review of non-technical loss detection methods," *Electr. Power Syst. Res.*, vol. 158, pp. 250–266, May 2018, doi: 10.1016/J.EPSR.2018.01.005.

[8] S. C. Yip, W. N. Tan, C. K. Tan, M. T. Gan, and K. S. Wong, "An anomaly detection framework for identifying energy theft and defective meters in smart grids," *Int. J. Electr. Power Energy Syst.*, vol. 101, pp. 189–203, Oct. 2018, doi: 10.1016/J.IJEPES.2018.03.025.

[9] F. Xiao and Q. Ai, "Electricity theft detection in smart grid using random matrix theory," *IET Gener. Transm. Distrib.*, vol. 12, no. 2, pp. 371–378, Jan. 2018, doi: 10.1049/IET-GTD.2017.0898;PAGE:STRING:ARTICLE/CHAPTER.

[10] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, "Electricity Theft Detection in Power Grids with Deep Learning and Random Forests," *J. Electr. Comput. Eng.*, vol. 2019, no. 1, p. 4136874, Jan. 2019, doi: 10.1155/2019/4136874.

[11] M. Nazmul Hasan, R. N. Toma, A. Al Nahid, M. M. Manjurul Islam, and J. M. Kim, "Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach," *Energies 2019, Vol. 12, Page 3310*, vol. 12, no. 17, p. 3310, Aug. 2019, doi: 10.3390/EN12173310.

[12] M. S. Saeed *et al.*, "Detection of Non-Technical Losses in Power Utilities—A Comprehensive Systematic Review," *Energies 2020, Vol. 13, Page 4727*, vol. 13, no. 18, p. 4727, Sep. 2020, doi: 10.3390/EN13184727.

[13] P. R. Jeyaraj, E. R. S. Nadar, A. C. Kathiresan, and S. P. Asokan, "Smart grid security enhancement by detection and classification of non-technical losses employing deep learning algorithm," *Int. Trans. Electr. Energy Syst.*, vol. 30, no. 9, p. e12521, Sep. 2020, doi: 10.1002/2050-7038.12521;ISSUE:ISSUE:DOI.

[14] S. O. Tehrani, M. H. Y. Moghaddam, and M. Asadi, "Decision Tree based Electricity Theft Detection in Smart Grid," *Proceeding 4th Int. Conf. Smart Cities, Internet Things Appl. SCIoT 2020*, pp. 46–51, Sep. 2020, doi: 10.1109/SCIOT50840.2020.9250194.

[15] M. S. Iqbal, S. Munawar, M. Adnan, A. Raza, M. A. Akbar, and A. Bermak, "A critical review of technical case studies for electricity theft detection in smart grids: A new paradigm based transformative approach," *Energy Convers. Manag. X*, vol. 26, p. 100965, Apr. 2025, doi: 10.1016/J.ECMX.2025.100965.

[16] A. Ullah, N. Javaid, M. Asif, M. U. Javed, and A. S. Yahaya, "AlexNet, AdaBoost and Artificial Bee Colony Based Hybrid Model for Electricity Theft Detection in Smart Grids," *IEEE Access*, vol. 10, pp. 18681–18694, 2022, doi: 10.1109/ACCESS.2022.3150016.

[17] M. Irfan *et al.*, "Energy Theft Identification Using Adaboost Ensembler in the Smart

Grids," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 2141–2158, Feb. 2022, doi: 10.32604/CMC.2022.025466.

[18] F. Shehzad, N. Javaid, S. Aslam, and M. Umar Javaid, "Electricity theft detection using big data and genetic algorithm in electric power systems," *Electr. Power Syst. Res.*, vol. 209, p. 107975, Aug. 2022, doi: 10.1016/J.EPSR.2022.107975.

[19] L. Wu, H. Shi, S. Fu, Y. Luo, and M. Xu, "p2Detect: Electricity Theft Detection With Privacy Preservation for Both Data and Model in Smart Grid," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2301–2312, May 2023, doi: 10.1109/TSG.2022.3214194.

[20] Z. Liu, W. Ding, T. Chen, M. Sun, H. Cai, and C. Liu, "A electricity theft detection method through contrastive learning in smart grid," *EURASIP J. Wirel. Commun. Netw. 2023 20231*, vol. 2023, no. 1, pp. 54-, Jun. 2023, doi: 10.1186/S13638-023-02258-Z.

[21] Pamir, N. Javaid, M. U. Javed, M. A. Houran, A. M. Almasoud, and M. Imran, "Electricity theft detection for energy optimization using deep learning models," *Energy Sci. Eng.*, vol. 11, no. 10, pp. 3575–3596, Oct. 2023, doi: 10.1002/ESE3.1541;WGROUP:STRING:PUBLICATION.

[22] A. I. Kawoosa, D. Prashar, M. Faheem, N. Jha, and A. A. Khan, "Using machine learning ensemble method for detection of energy theft in smart meters," *IET Gener. Transm. Distrib.*, vol. 17, no. 21, pp. 4794–4809, Nov. 2023, doi: 10.1049/GTD2.12997;WGROUP:STRING:PUBLICATION.

[23] H. Iftikhar *et al.*, "Electricity theft detection in smart grid using machine learning," *Front. Energy Res.*, vol. 12, p. 1383090, Mar. 2024, doi: 10.3389/FENRG.2024.1383090/TEXT.

[24] A. Ullah, I. U. Khan, M. Z. Younas, M. Ahmad, and N. Kryvinska, "Robust resampling and stacked learning models for electricity theft detection in smart grid," *Energy Reports*, vol. 13, pp. 770–779, Jun. 2025, doi: 10.1016/J.EGYR.2024.12.041.

[25] S. Nirmal, P. Patil, and J. R. R. Kumar, "CNN-AdaBoost based hybrid model for electricity theft detection in smart grid," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 7, p. 100452, Mar. 2024, doi: 10.1016/J.PRIME.2024.100452.

[26] S. A. Abro *et al.*, "Non-technical loss detection in power distribution networks using machine learning," *Sci. Rep.*, vol. 15, no. 1, pp. 36189-, Dec. 2025, doi: 10.1038/S41598-025-20048-Z;SUBJMETA.

[27] S. Kim *et al.*, "Data-Driven Approaches for Energy Theft Detection: A Comprehensive Review," *Energies 2024, Vol. 17, Page 3057*, vol. 17, no. 12, p. 3057, Jun. 2024, doi: 10.3390/EN17123057.

[28] P. M. Kgaphola, S. M. Marebane, and R. T. Hans, "Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review," *Electr. 2024, Vol. 5, Pages 334-350*, vol. 5, no. 2, pp. 334–350, Jun. 2024, doi: 10.3390/ELECTRICITY5020017.

Copyright © by authors and 50Sea. This work is licensed under Creative Commons Attribution 4.0 International License.