



International Journal of Agriculture Extension and Social Development

ISSN Print: 2618-0723
 ISSN Online: 2618-0731
 NAAS Rating (2026): 5.04
 IJAESD 2026; 9(9): 833-836
www.extensionjournal.com
 Received: 26-06-2026
 Accepted: 10-08-2026
 Published: 23-09-2026

Vijeta Pal

Alumna, Department of
 Electrical Engineering,
 GBPUA&T, College of
 Technology, Pantnagar
 University, Uttarakhand, India

Sandeep Kumar Goel

Professor, Department of
 Electrical Engineering,
 GBPUA&T, College of
 Technology, Pantnagar
 University, Uttarakhand, India

IoT-enabled monitoring of electrical power systems over computer networks: An edge-to-cloud architecture for real-time measurement, event detection and secure remote supervision

Vijeta Pal¹, Sandeep Kumar Goel²

DOI: <https://www.doi.org/10.33545/26180723.2026.v9.i9k.4277>

ABSTRACT

The increasing penetration of distributed energy resources, power electronic loads, industrial automation and geographically dispersed electrical assets has created a need for continuous and network-accessible power-system monitoring. Conventional monitoring approaches are frequently dependent on local instruments or supervisory control and data acquisition infrastructure that may provide limited accessibility, heterogeneous interfaces and delayed fault information. This paper proposes an Internet of Things (IoT)-enabled monitoring architecture in which electrical measurements are acquired at the edge, normalized by a gateway, transported through an IP computer network and presented through a remote supervisory dashboard. The proposed architecture combines voltage, current, active power, reactive power, power factor, frequency and energy measurements with event-based monitoring. Modbus/TCP is considered for field-device integration, MQTT for lightweight telemetry, and TLS-secured IP communication for remote data transfer. Network segmentation using VLANs and quality-of-service principles is incorporated to improve reliability and isolate monitoring traffic from general-purpose traffic. A rule-based anomaly layer is also proposed for identifying overvoltage, undervoltage, overcurrent, frequency deviation and communication-loss events. A reproducible simulation-oriented validation methodology is defined to evaluate measurement transmission, event detection and communication performance without claiming unverified field results. The work demonstrates how electrical engineering and computer networking can be integrated into a scalable monitoring framework suitable for distribution panels, transformers, industrial feeders and smart-grid laboratory environments.

Keywords: Internet of Things, Electrical power system, Power monitoring, Computer network, MQTT, Modbus/TCP, Edge computing, Smart grid, Power quality, Remote monitoring, VLAN, Cybersecurity

1. Introduction

Electrical power systems are evolving from isolated, centrally supervised infrastructures toward highly connected cyber-physical systems. Smart-grid technologies increasingly use communication networks to observe, coordinate and optimize generation, transmission, distribution and consumption. IoT provides a practical mechanism for connecting electrical sensors, intelligent electronic devices, meters and edge controllers to local and remote information systems. Recent research has demonstrated IoT-based transformer monitoring, power-quality monitoring and smart-grid fault-detection applications, confirming the value of real-time remote visibility.

Despite this progress, many low- and medium-scale monitoring implementations focus primarily on sensor acquisition and cloud visualization. The computer-network layer is often treated as a transparent transport mechanism rather than as an engineering component that must be designed for segmentation, latency, reliability, cybersecurity and interoperability. For electrical engineering applications, this is a significant gap because a monitoring system must preserve measurement integrity while operating over heterogeneous Ethernet/IP networks.

This paper therefore treats the electrical measurement chain and the computer network as a single integrated monitoring system. The proposed architecture contains four logical layers: (i) electrical sensing and metering, (ii) edge acquisition and protocol conversion, (iii) IP-network transport and security, and (iv) analytics and visualization. The main contributions are: a protocol-interoperable edge-to-cloud architecture; explicit integration of VLAN-based network segmentation and MQTT/Modbus-TCP communication; an event-detection mechanism for electrical abnormalities and communication loss; and a reproducible validation methodology suitable for laboratory or simulation-based implementation.

The work is intentionally written as a design-and-validation manuscript. Numerical performance values should be replaced by measured values from the author's testbed before submission as experimental results. This avoids presenting fabricated field measurements as original observations.

Corresponding Author: Vijeta Pal

Alumna, Department of
 Electrical Engineering,
 GBPUA&T, College of
 Technology, Pantnagar
 University, Uttarakhand,
 India

2. Related work

IoT has been increasingly applied to electrical infrastructure because low-cost sensors and networked controllers can provide continuous measurements and remote alarms. A 2025 study on a 100 kVA distribution transformer combined sensors, local logging, GSM notifications and the ThingSpeak IoT platform for real-time monitoring and fault reporting. The work illustrates the practical benefit of connecting electrical condition monitoring to communication services.

Recent work has also investigated IoT-assisted transmission-line fault classification using virtual phasor measurement units and machine-learning techniques. Such approaches indicate that IoT can extend beyond simple measurement display toward intelligent event analysis. In addition, recent reviews of IoT in smart grids emphasize that IoT can support monitoring, control and optimization but introduce challenges related to interoperability, reliability and cyber-physical security.

The research gap addressed here is the integration of electrical measurement, IP-network engineering and edge/cloud monitoring into a single practical architecture. Rather than proposing an isolated sensor node, the paper emphasizes the network path from electrical device to gateway, switch/router, broker and dashboard. This enables electrical engineers to evaluate not only measurement accuracy but also communication availability and network behavior.

Layer	Main Components	Typical Protocols	Primary Function
Electrical/Field	PT/CT or isolated sensors, smart meter, relay	Modbus RTU, pulse, analog	Measure electrical parameters
Edge	PLC/RTU/industrial PC/IoT gateway	Modbus/TCP, MQTT client	Acquire, validate and normalize data
Network	Ethernet switch, router/firewall, monitoring VLAN	IPv4, TCP/IP, VLAN, QoS	Reliable and segmented transport
Application	MQTT broker, database, analytics, dashboard	MQTT, HTTPS/TLS, SQL	Store, analyze, visualize and alert

4. Electrical measurement model

For a balanced or unbalanced three-phase system, phase voltages and currents are acquired independently whenever possible. For each phase k , the instantaneous RMS voltage and current are represented by V_k and I_k . Active power is calculated from the voltage-current relationship and power factor. For a balanced system, the three-phase active power can be approximated by $P = \sqrt{3} V_{LL} I_L \cos(\phi)$, where V_{LL} is line-to-line RMS voltage, I_L is line current and ϕ is the phase angle.

The apparent power is $S = \sqrt{3} V_{LL} I_L$, while reactive power can be obtained from $Q = \sqrt{(S^2 - P^2)}$ when the measurement conditions permit. Power factor is $PF = P/S$. Energy is obtained by integrating active power over time, $E(t) = \int P(t) dt$. In an implementation, meter-reported values should normally be preferred over recomputing quantities when the meter has certified measurement algorithms.

Electrical limits are application dependent. For example, an operator may define undervoltage, overvoltage, overcurrent and frequency thresholds according to the applicable grid code, equipment rating and protection philosophy. The monitoring system must distinguish between an informational alarm and a protection action; the proposed IoT layer is a monitoring and supervisory system and should not replace certified protection relays.

5. Computer network design

A reliable monitoring network should use deterministic addressing, documented device identities and logical segmentation. The recommended topology is: smart meter/sensors → edge gateway → access switch → monitoring VLAN → Layer-3 gateway/firewall → MQTT broker/application server. Where multiple electrical sites are involved, site-to-site VPN or another approved secure WAN mechanism can connect remote gateways to a central monitoring platform.

3. Proposed system architecture

The proposed architecture is organized into four layers. At the field layer, electrical sensors or smart meters measure voltage, current, frequency, active power, reactive power, apparent power, power factor and accumulated energy. An edge controller or industrial gateway collects these measurements. The gateway may use Modbus RTU/RS-485, Modbus/TCP, Ethernet, or a meter-specific protocol on the field side.

At the network layer, the gateway connects to an Ethernet switch. A dedicated monitoring VLAN is recommended so that measurement traffic is logically separated from office or user traffic. A Layer-3 gateway provides controlled routing toward the IoT broker or application server. MQTT is used as the preferred telemetry protocol because its publish/subscribe model reduces coupling between measurement producers and monitoring applications.

At the application layer, an MQTT broker receives timestamped telemetry. A database stores historical measurements and an analytics service evaluates threshold and communication events. A dashboard displays real-time values, trends and alarms. The architecture can be deployed on-premises or connected to a cloud service depending on the required availability and security policy.

VLAN segmentation reduces unnecessary broadcast exposure and provides a boundary between operational monitoring devices and general enterprise endpoints. Access-control rules should allow only the required traffic, such as Modbus/TCP between the gateway and meter, MQTT from gateway to broker, and HTTPS from authorized users to the dashboard. Management protocols should be separated from measurement traffic where practical.

Network performance can be quantified using end-to-end latency, packet-loss ratio, telemetry delivery ratio and broker availability. For N transmitted telemetry messages, the packet-loss ratio is $L = \frac{N - N_r}{N} \times 100\%$, where N_r is the number of messages received. Average application latency is computed from timestamp pairs after accounting for clock synchronization. These metrics allow the electrical monitoring system to be evaluated as a communication system rather than merely as a sensor project.

6. IoT communication and data flow

The edge gateway publishes telemetry using an MQTT topic hierarchy such as power/site01/feeder01/voltage, power/site01/feeder01/current and power/site01/feeder01/alarm. Payloads should include a timestamp, device identifier, measurement value, engineering unit and quality/status field. A compact JSON payload can be used where bandwidth permits.

MQTT Quality of Service should be selected according to the operational requirement. QoS 0 minimizes overhead but does not guarantee delivery; QoS 1 supports at-least-once delivery and therefore requires duplicate handling at the application layer; QoS 2 provides stronger delivery semantics with additional overhead. For many monitoring systems, QoS 1 combined with message identifiers and timestamps is a practical compromise.

Transport security should use TLS with authenticated credentials or certificates. Broker authorization should restrict each gateway to its

permitted topics. Credentials must not be embedded as plaintext in source code or configuration files that are accessible to ordinary users. Time synchronization using NTP or an equivalent mechanism is recommended because accurate timestamps are essential for event correlation.

7. Fault and anomaly detection

The proposed edge/application analytics layer uses two complementary mechanisms. First, deterministic rules detect events that have clear engineering definitions. Examples include voltage below $V_{\min}$, voltage above $V_{\max}$, current above $I_{\max}$, frequency outside the permitted band, power factor below $PF_{\min}$ and absence of telemetry for more than T_{timeout} .

Second, a data-quality layer identifies communication anomalies. A stale timestamp, repeated identical measurement, invalid sensor status, excessive message delay or sudden loss of heartbeat is classified as a communication/data-quality event rather than an electrical fault. This distinction prevents a network outage from being incorrectly interpreted as zero electrical load.

For future work, the deterministic layer can be extended with statistical or machine-learning methods. Rolling mean, standard deviation, exponentially weighted moving averages and isolation-based anomaly detection can identify abnormal behavior without requiring a fixed threshold for every operating condition. Any machine-learning result should be validated against labeled electrical events before being used for operational decision-making.

Metric	Test condition	Expected/target	Measured value	Observation
Telemetry delivery ratio	Normal network	$\geq 99\%$ target	[Insert]	[Insert]
Average end-to-end latency	Normal network	Application dependent	[Insert]	[Insert]
Alarm detection time	Electrical threshold event	Near real-time	[Insert]	[Insert]
Recovery time	Gateway/broker interruption	Application dependent	[Insert]	[Insert]
Packet-loss ratio	Controlled impairment	Record actual	[Insert]	[Insert]

The most important discussion should relate network behavior to electrical monitoring quality. A small amount of packet loss may be tolerable for slow-changing energy measurements but unacceptable for high-frequency event streams. Similarly, a dashboard that appears operational can still contain stale measurements if the application does not expose data age. Therefore, the proposed system reports both value and data quality, enabling the operator to distinguish a genuine electrical state from a communication artifact.

Scalability should also be considered. Increasing the number of meters increases message volume and database writes. Topic design, batching, message frequency and broker capacity should be evaluated before deployment. Edge aggregation can reduce bandwidth by publishing slow-changing parameters at lower frequency while sending event messages immediately.

10. Cybersecurity considerations

Electrical monitoring systems are cyber-physical systems and should be protected against unauthorized access and manipulation. Recommended controls include network segmentation, least-privilege firewall rules, TLS encryption, unique device credentials, certificate-based authentication where feasible, secure firmware management, logging, time synchronization and regular backup of configuration data.

The monitoring architecture should follow a defense-in-depth model. A compromise of a dashboard user account should not provide direct access to field devices. Likewise, a field gateway should not be allowed to communicate with unrelated enterprise systems. Where an electrical control function is required, it should be isolated and governed by an appropriate OT security architecture; monitoring traffic

8. Validation methodology

The proposed validation is designed to be reproducible in a laboratory, digital twin or network emulator. The electrical side can be represented by a programmable source, power meter or simulated feeder. The communication side can be implemented using an Ethernet switch, an IoT gateway and an MQTT broker. A network emulator can introduce controlled latency, packet loss and link interruption to evaluate communication robustness.

Three test groups are recommended. Test Group A validates measurement transport under normal operation. Test Group B introduces electrical events such as undervoltage, overcurrent and frequency deviation. Test Group C introduces communication disturbances such as packet loss, increased latency, gateway restart and broker unavailability. For every test, the raw measurement, gateway timestamp, broker timestamp, event classification and recovery time should be stored.

A publication-ready experimental paper should report the actual sample count, measurement instrument model, calibration status, sampling interval, network topology, switch model, gateway hardware, broker software, operating-system version and test duration. These details are essential for reproducibility.

9. Results and discussion

The following table is intentionally provided as a measurement template. Values must be populated from the author's actual laboratory or simulation runs before submission. The manuscript should not claim the placeholder values as experimental findings.

should not be given unrestricted write access to protection or control equipment.

11. Practical implementation example

A representative laboratory implementation can use a three-phase smart meter connected to an industrial gateway through RS-485/Modbus RTU or Ethernet/Modbus TCP. The gateway connects to a managed Ethernet switch using a dedicated access port in the monitoring VLAN. The Layer-3 gateway forwards only authorized MQTT and management traffic to an on-premises or cloud broker. A dashboard displays V, I, P, Q, PF, frequency and energy, while an alarm service records threshold crossings and communication failures.

The design can be adapted to transformer monitoring, industrial distribution boards, solar photovoltaic plants, microgrids, building energy systems and electrical laboratories. The same computer-network principles remain applicable even when the electrical equipment changes.

12. Advantages and limitations

The principal advantages are remote visibility, protocol interoperability, centralized historical storage, event-based notification, network segmentation and scalability. The architecture also creates a clear interface between electrical engineering measurements and computer-network services.

The principal limitation is that IoT communication cannot guarantee electrical protection performance. Network delay, broker failure or gateway failure can make remote data temporarily unavailable. Therefore, local protection and interlocking must remain independent of the IoT monitoring path. A second limitation is that the proposed

manuscript does not claim a specific measured accuracy or network performance until the author's test data are inserted.

13. Conclusion

This paper presented an IoT-enabled architecture for monitoring electrical power systems through computer networks. The proposed edge-to-cloud framework integrates electrical measurement, Modbus/TCP or equivalent field communication, Ethernet/IP networking, VLAN segmentation, MQTT telemetry, secure remote access and event analytics. The architecture is intended to provide a practical bridge between electrical engineering and modern computer networking.

The key engineering principle is that an IoT power-monitoring system should be evaluated as both an electrical measurement system and a communication system. Measurement correctness, data freshness, packet delivery, network security and event detection must be considered together. Future work will focus on a hardware-in-the-loop implementation, long-duration field measurements, power-quality indices, adaptive anomaly detection and quantitative comparison of wired Ethernet, Wi-Fi and cellular communication paths.

Submission Note

This manuscript is a publication-oriented draft. A journal with a NAAS score above 7 should be selected only after checking the current official NAAS list, scope, indexing, article-processing charges, and submission requirements. NAAS score is a property of the journal, not a guarantee that an individual paper will be accepted. Before submission, replace all [Insert] fields with original experimental/simulation results, add author affiliations and ORCID details, prepare figures and a graphical system architecture, and perform plagiarism/similarity and reference-format checks.

References

1. National Academy of Agricultural Sciences (NAAS). NAAS Score of Science Journals – Effective from January 1, 2026. official journal list. 2026.

2. Nkinyam CM, Encho LT, Mbaka NE. Design and implementation of a 100 kVA transformer monitoring and fault detection system for distribution network. *Journal of Electrical Systems and Information Technology*. 2025;12:21.
3. Alsafran AS, Alwabari M, Al-Bahrani M. Challenges in Implementing IoT for Enhanced Reliability and Effectiveness in Smart Grids: Literature Review. *International Transactions on Electrical Energy Systems*. 2025.
4. Delfianti R, Tazayul VA, Mustaqim B, Nussyura F, Harsito C. Internet of Things (IoT) Based Electrical Power Monitoring System for Solar Power Plants Using the Telegram Application. *Vokasi UNESA Bulletin of Engineering, Technology and Applied Science*. 2025;2(3):428-443.
5. Raja S, Halim M, Othman M, Jali M. Design and Development of Wi-Fi and GPS-Based Smart Monitoring and Fault Detection System for Three-Phase Power Transmission Line Using Arduino. *Journal of Power and Energy Engineering*. 2025;13:343-370.
6. OASIS Open. MQTT Version 5.0, OASIS Standard. 2019.
7. Modbus Organization. MODBUS Application Protocol Specification. Modbus.org.
8. IEEE. IEEE Std 802.1Q, Bridges and Virtual Bridged Local Area Networks.
9. IEEE. IEEE Std 519, IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems.
10. International Electrotechnical Commission. IEC 61850, Communication Networks and Systems for Power Utility Automation.

How to cite this article: Pal V, Goel SK. IoT-enabled monitoring of electrical power systems over computer networks: An edge-to-cloud architecture for real-time measurement, event detection and secure remote supervision. *International Journal of Agriculture Extension and Social Development*. 2026;9(9):833-836. doi: <https://www.doi.org/10.33545/26180723.2026.v9.i9k.4277>