Journal of Computer Technology and Software

ISSN:2998-2383

Vol. 5, No. 3, 2026

An IoT-Based Solution for Power Information Acquisition and Remote Monitoring

Théon Valcourt
University of Windsor, Windsor, Canada
tvalcourt090@uwindsor.ca

Abstract: To improve the real-time monitoring capability and management efficiency of power systems, this paper investigates a solution for power information acquisition and remote monitoring based on Internet of Things (IoT) technology. By conducting an in-depth analysis of the core components of IoT architecture and integrating the characteristics of power data, appropriate sensor technologies and communication protocols are selected and optimized. A remote monitoring system architecture is designed, consisting of a data center, user interface, and corresponding security mechanisms. In practical applications, the proposed solution effectively acquires power system data and performs real-time analysis, thereby enabling efficient remote monitoring of power systems. Experimental results demonstrate that IoT technology exhibits significant application potential in power information acquisition and remote monitoring, providing essential technical support for the modernization of power industry management.

Keywords: Internet of Things (IoT), power information acquisition, remote monitoring, sensors, data transmission

1. Introduction

Power, as the foundation of modern society, plays a crucial role in ensuring social and economic development through its safety, efficiency, and stable operation. With the continuous advancement of technology, how to utilize advanced technologies to guarantee the efficient and stable operation of power systems has become a common concern in both industry and academia. Among these technologies, the Internet of Things (IoT), with its extensive sensing, networking, and processing capabilities, provides new possibilities for power information acquisition and remote monitoring.

2. Related work

Modern intelligent systems, particularly cloud platforms and distributed microservice architectures, are increasingly characterized by high-dimensional data, dynamic workloads, and complex inter-component dependencies. Recent advances in large language models (LLMs) have demonstrated strong capabilities in abstraction, reasoning, and controllable generation, enabling more flexible representations of complex system behaviors [1]. Meanwhile, the evolution of large-scale cyber-physical infrastructures, such as smart grids, highlights the importance of reliable communication and data integration in complex systems [2][4]. These developments share common challenges in system observability, scalability, and robustness under dynamic environments.

The proliferation of Internet of Things (IoT) technologies further amplifies system complexity by introducing massive heterogeneous data sources and tightly coupled sensing-communication-computation pipelines [6][9]. Such environments exhibit strong temporal dynamics and structural dependencies, making traditional rule-based or static statistical approaches insufficient for modeling system behavior. Early communication and sensing paradigms, including wireless sensor networks, laid the foundation for distributed data acquisition and monitoring in large-scale systems [14][17]. Subsequent standardization efforts and protocol designs for IoT systems further enabled scalable and interoperable system architectures [19][22].

In cloud and microservice platforms, anomaly detection has become a critical task for ensuring system reliability and performance stability. Recent studies have explored graph-based representation learning to capture structural relationships among services and resources, improving the ability to detect performance anomalies in complex environments [3]. Similarly, graph-transformer architectures have been proposed to model dependency-coupled systems and reconstruct system states for unsupervised anomaly detection [5]. These approaches highlight the importance of jointly modeling temporal evolution and structural dependencies in modern distributed systems.

To address dynamic resource allocation and system control, reinforcement learning (RL) and multi-agent learning methods have been increasingly adopted. For example, multi-objective adaptive rate limiting mechanisms leverage deep reinforcement learning to balance system performance and resource utilization in microservices [7]. In financial and transaction systems, federated learning approaches further extend anomaly detection capabilities by enabling collaborative modeling across distributed data sources while preserving privacy [8]. These trends indicate a shift toward more adaptive and decentralized learning paradigms in complex systems.

Recent work also integrates semantic modeling and retrieval-augmented learning to enhance anomaly detection in evolving data environments. Context-aware deep anomaly detection frameworks combine retrieval mechanisms with learned representations to improve detection accuracy under data drift and distribution shifts [10]. In parallel, system-level optimization techniques such as token-level GPU scheduling have been proposed to improve resource efficiency for large-scale model serving, highlighting the interplay between system performance and intelligent scheduling [11]. Moreover, advances in LLM-based agent systems enable compositional reasoning and zero-shot task generalization, further extending the applicability of AI in complex decision-making scenarios [12].

Causal reasoning and uncertainty modeling have emerged as important directions for improving interpretability and robustness. For instance, uncertainty-aware decision-making frameworks have been applied to marketing attribution and budget optimization, enabling more reliable decision support under noisy environments [13]. Similarly, causal reasoning over knowledge graphs provides a structured approach for understanding intervention effects and system behavior changes [21]. These methods are particularly relevant for anomaly detection tasks where distinguishing root causes from correlated signals is essential.

In large-scale distributed systems, adaptive control mechanisms such as predictive autoscaling incorporate uncertainty quantification to improve system stability under varying workloads [15]. Meta-learning-based approaches further enhance anomaly detection by enabling rapid adaptation to new system conditions and unseen anomaly patterns [16]. In financial and decision systems, multi-agent reinforcement learning has also been applied to optimize dynamic strategies under risk constraints, demonstrating strong capability in handling complex optimization problems [18].

Finally, recent research has emphasized the importance of causal representation learning for improving interpretability and robustness in anomaly detection and risk analysis. By integrating structural modeling with causal inference, these approaches enable systems to move beyond correlation-based detection toward mechanism-aware analysis [23]. This shift is particularly important in cloud computing environments, where system behaviors are driven by complex interactions among resources, services, and workloads.

3. Main Technical Components of the Internet of Things

The IoT technical system is the result of multi-layer and multi-domain integration, as illustrated in Figure 1. Its primary technical components include:

Sensor technology-As the data source of the IoT, sensors are capable of perceiving, capturing, and transforming information from the physical world into digital signals.

Communication technology-This ensures efficient and reliable data transmission from source nodes to destination nodes, covering both wired and wireless communication methods, such as NFC, RFID, LoRa, and 5G.

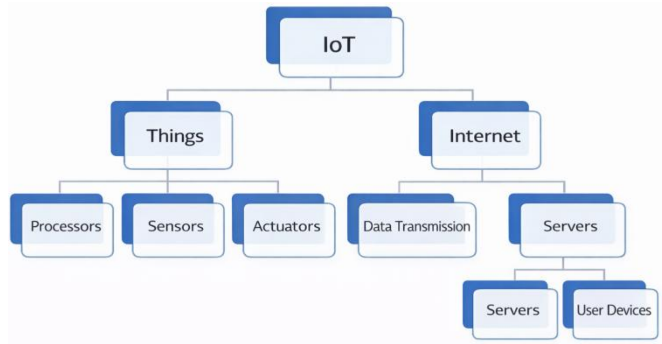

Figure 1. Technical Architecture of the Internet of Things

Data processing and storage technology-Given the massive amount of data generated by IoT systems, big data technologies are required for storage, analysis, and mining to extract valuable insights.

Network security technology-Due to the openness and cross-domain characteristics of IoT systems, network security is particularly critical to ensure data integrity, privacy protection, and overall system stability.

Edge computing technology-Considering the wide distribution of IoT devices, edge computing enables rapid data processing near the devices, thereby reducing latency and improving response speed.

Cloud platforms provide powerful computing capabilities, data storage, and service deployment support for IoT systems [24]. Meanwhile, with the increasing complexity of Industrial IoT environments, data quality issues such as imbalance and sparsity have become critical challenges for reliable system monitoring. To address these problems, Huang et al. proposed a self-supervised learning-based framework for stable fault diagnosis, which can effectively learn robust feature representations from unlabeled and imbalanced data, thereby improving diagnostic accuracy and system stability [25]. This line of research highlights the importance of incorporating advanced data-driven learning strategies into IoT-based power monitoring systems, particularly for enhancing anomaly detection and intelligent analysis under real-world conditions.

4. Research on Power Information Acquisition Technology

4.1 Characteristics and Classification of Power Data

As the core information carrier in power grid systems, power data exhibit unique characteristics and classification methods.

From a characteristics perspective, power data are typically high-frequency, real-time, large-scale, and multi-dimensional. Due to the continuous operation of power systems, data are generated at high frequency and must be collected in real time to ensure system stability.

Meanwhile, the increasing number of sensors and measurement devices has led to rapid growth in data volume and diversity. From a classification perspective, power data can be categorized as follows:

Operational data-Including voltage, current, frequency, etc., which directly reflect the operating status of the power grid.

Fault data-Comprising various parameters and waveforms recorded during grid faults, which are crucial for fault diagnosis.

Status data-Describing equipment health conditions, such as transformer oil temperature and insulation status.

User data-Involving electricity consumption, usage time, and load characteristics of power users, which provide guidance for demand-side management and electricity pricing strategies.

4.2 Sensor Technology and Selection

Sensor technology plays a critical role in power information acquisition systems, providing first-hand raw data for power system monitoring and analysis. With advancements in electronic technology and material science, modern sensors feature higher precision, smaller size, and stronger anti-interference capability. In power systems, commonly used sensors include voltage sensors, current sensors, temperature sensors, and vibration sensors, which perform real-time monitoring of different electrical parameters [26].

From a modeling perspective, the basic measurement relationship of a sensor can be expressed as:

$$y(t) = kx(t) + b$$

where $x(t)$ represents the measured physical quantity, $y(t)$ denotes the sensor output signal, k is the sensitivity coefficient, and b is the offset error.

To evaluate measurement accuracy, the relative measurement error can be defined as:

$$\varepsilon = \frac{|x_m - x_r|}{x_r}$$

where x_m is the measured value and x_r is the reference value. Minimizing ε is essential to ensure reliable system operation.

When selecting appropriate sensors, several key factors must be considered:

Measurement range and accuracy-The selected sensor must satisfy practical measurement requirements in terms of precision and dynamic range.

Environmental adaptability-Since power systems may operate in harsh environments, sensors must possess strong anti-interference capability and environmental tolerance.

Installation and maintenance-Easy installation and convenient maintenance can significantly reduce operational costs.

Economic efficiency-Under the premise of meeting technical requirements, cost-effectiveness remains an important consideration.

Additionally, sensor reliability over time can be modeled using an exponential reliability function:

$$R(t) = e^{-\lambda t}$$

where λ represents the failure rate and t denotes operating time. Higher reliability corresponds to smaller failure rates, which is critical for long-term stable operation of power monitoring systems.

4.3 Data Transmission and Communication Protocols

In power information acquisition systems, data transmission constitutes one of the core components, ensuring smooth and real-time information flow from sensors to data centers. To guarantee data integrity, security, and transmission efficiency, specialized communication protocols are designed and implemented. These protocols define data encoding, transmission, and decoding mechanisms, while also addressing error detection, data synchronization, and flow control.

The transmission delay can be generally modeled as:

$$T_{total} = T_{prop} + T_{trans} + T_{proc}$$

where T_{prop} denotes propagation delay, T_{trans} represents transmission delay, and T_{proc} is processing delay. Minimizing T_{total} is essential for meeting real-time monitoring requirements.

In the power industry, commonly adopted communication protocols include IEC 61850, Modbus, and DNP3. These protocols are designed to provide high reliability and low-latency communication services tailored to power system applications. For example, IEC 61850 is a standard specifically developed for power system automation, supporting interoperability across multiple hardware devices and system platforms. DNP3 is widely used in distributed networks, offering a robust and scalable communication framework.

The selection of an appropriate communication protocol should consider system scale, real-time requirements, security constraints, and future scalability. While ensuring reliable data transmission, the chosen protocol should also minimize its impact on existing networks to optimize resource utilization and maintain stable power system operation.

5. Remote Monitoring System Architecture

5.1 Overall Design and Architecture Overview

Figure 2 illustrates the architecture of the remote monitoring system. Based on the four-layer IoT framework, the system is organized into the perception layer, transmission layer, service layer, and application layer from bottom to top.

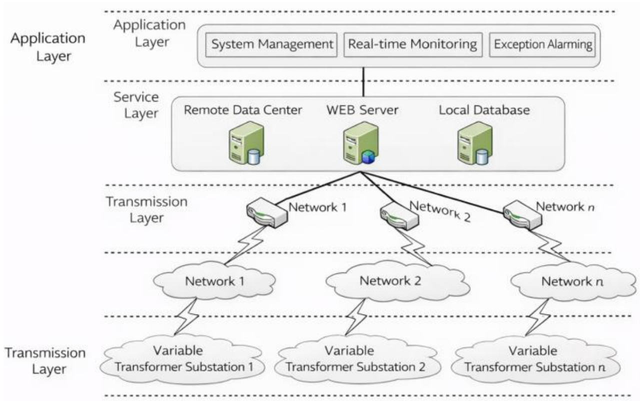

Figure 2. Remote Monitoring System Architecture

The perception layer consists of various sensors and terminal devices deployed across power facilities. These devices continuously monitor operational states and convert physical parameters into transmittable electronic data.

The transmission layer is responsible for securely and efficiently delivering the collected data to the data center through multiple communication technologies-including wired, wireless, and optical fiber networks.

At the service layer, data are not only stored efficiently but also undergo preliminary cleansing, integration, and analysis to provide structured and meaningful information support for upper-layer applications.

The application layer offers intuitive user interfaces and service functions, enabling real-time monitoring of equipment status, historical data review, and alarm notifications. It further supports advanced analytics and decision-making processes [27]. In addition, the application layer provides extended services related to power system operations, such as remote control and fault prediction.

5.2 Data Center and Cloud Storage Design

n modern remote monitoring systems, the data center and cloud storage constitute critical components for ensuring data security, reliability, and high-efficiency processing. As the core of the service layer within the IoT architecture, the data center must exhibit high scalability, backup capability, redundancy, and fault-switching mechanisms to meet increasing computational demands.

Cloud storage provides a flexible and scalable data solution. By integrating distributed file systems and object storage technologies, it ensures data integrity and security while supporting real-time data processing and analytics. Through the adoption of big data processing frameworks such as Apache Kafka and Apache Spark, the data center can capture and analyze data streams in real time, thereby delivering timely feedback to the application layer [28].

To further safeguard data privacy and security, multiple protection mechanisms must be implemented, including data encryption, access control strategies, and Secure Sockets Layer-SSL-transmission protocols.

5.3 User Interface and Interaction Design

In remote monitoring system development, user interface and interaction design are particularly important because they directly affect user experience and operational efficiency. An effective interface should provide intuitive visualization, concise layouts, and comprehensive functionality, allowing users to quickly understand and operate system features without requiring deep knowledge of underlying technical details.

Interaction design should consider user behavior patterns and application scenarios. For example, frequently used functions may be provided with shortcut access, or intelligent recommendations may be generated based on user operation patterns.

Furthermore, to accommodate diverse user groups and device environments, the interface should possess strong responsiveness and adaptability, ensuring consistent user experience across different devices and screen sizes [29].

6. Application Case of IoT in Power Monitoring

6.1 Case Introduction

In recent years, a municipal power supply company launched a project entitled "Smart Energy Management System," aiming to enhance grid efficiency and reliability through IoT technologies. Sensors were deployed at critical nodes to collect voltage, current, power, and other related parameters in real time.

These data were transmitted to the data center via the IoT transmission layer and processed using advanced big data analytics and artificial intelligence techniques. As a result, the operation team obtained real-time energy usage information, fault alerts, and optimization recommendations, significantly improving operational management capabilities.

6.2 Implementation Process and Technical Challenges

During the implementation of the Smart Energy Management System project, several technical challenges significantly influenced project progress.

First, at the perception layer, selecting high-precision sensors suitable for complex power environments and ensuring stable operation presented a major challenge. To obtain accurate current, voltage, and frequency measurements, sensors were required to exhibit strong anti-interference capability and low error rates.

Second, at the transmission layer, the complexity and wide distribution of power infrastructure required reliable, real-time, and secure long-distance data transmission to central servers. The project adopted high-speed, low-latency communication protocols such as MQTT; however, network instability and cybersecurity threats remained concerns.

Third, at the service layer, processing, storing, and analyzing large volumes of real-time data demanded high-performance computing capabilities and advanced data processing technologies. Distributed databases and stream-processing frameworks were implemented to address these requirements, although real-time synchronization and data consistency remained ongoing challenges.

Finally, at the application layer, providing operators with intuitive and easy-to-understand data visualization interfaces while satisfying operational demands was critical. The accuracy of backend data analytics algorithms and models directly influenced system reliability.

6.3 Performance Evaluation

According to Table 1, after introducing IoT technology, the Smart Energy Management System achieved significant improvements in monitoring efficiency and accuracy. Data acquisition latency decreased from 15 s to 5 s, enhancing system responsiveness. Data transmission failure rates were reduced from 3.5% to 0.8%, strengthening operational stability.

Table 1: Project Implementation Results

Evaluation Metric	Before Application	After Application	Improvement Percentage (%)
Data Acquisition Latency (s)	15	5	−66.7
Data Transmission Failure Rate (%)	3.5	0.8	−77.1
Fault Detection Response Time (min)	30	5	−83.3
User Satisfaction (Score, out of 10)	6.5	9.2	41.5
System Operational Stability (d)	30	60	100

Fault detection response time was substantially shortened from 30 min to 5 min, enabling rapid fault localization and resolution. User satisfaction increased from 6.5 to 9.2, reflecting high acceptance of the upgraded system. Moreover, stable system operation duration doubled from 30 d to 60 d.

These results demonstrate that IoT-based solutions significantly enhance power monitoring performance and user satisfaction.

7. Conclusion

The development of IoT technology has brought transformative changes to the power industry, particularly in power information acquisition and remote monitoring. This study analyzed the application of IoT in power monitoring and highlighted its core value in improving real-time performance, accuracy, and system stability. The integration of IoT technology significantly reduces human error and provides strong technical support for stable power system operation.

With continuous technological innovation, IoT is expected to play an increasingly important role in the modernization and intelligent transformation of the power industry, promoting the development of more efficient, secure, and environmentally sustainable power systems.

References

[1] X. Song, Y. Liu, Y. Luan, J. Guo and X. Guo, "Controllable abstraction in summary generation for large language models via prompt engineering," arXiv preprint arXiv:2510.15436, 2025.

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529-539, 2011.

[3] Y. Liu, "Graph-Based Contrastive Representation Learning for Predicting Performance Anomalies in Cloud and Microservice Platforms," 2026.

[4] X. Fang, S. Misra, G. Xue and D. Yang, "Smart grid — The new and improved power grid: A survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, 2011.

[5] C. Zhang, C. Shao, J. Jiang, Y. Ni and X. Sun, "Graph-Transformer Reconstruction Learning for Unsupervised Anomaly Detection in Dependency-Coupled Systems," 2025.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[7] N. Lyu, Y. Wang, Z. Cheng, Q. Zhang and F. Chen, "Multi-Objective Adaptive Rate Limiting in Microservices Using Deep Reinforcement Learning," Proceedings of the 4th International Conference on Artificial Intelligence and Intelligent Information Processing, pp. 862-869, Oct. 2025.

[8] H. Feng, Y. Wang, R. Fang, A. Xie and Y. Wang, "Federated risk discrimination with siamese networks for financial transaction anomaly detection," Proceedings of the 2025 2nd International Conference on Digital Economy and Computer Science, pp. 231-236, Oct. 2025.

[9] T. Ahmad and D. Zhang, "Using the internet of things in smart energy systems and networks," Sustainable Cities and Society, vol. 68, Art. no. 102783, 2021.

[10] N. Chen, Y. Zhang, W. Wang, Z. Pan, Y. Wang and Y. Lu, "CoReAD: Context-Aware Retrieval-Augmented Deep Anomaly Detection for Evolving Business Tabular Data."

[11] H. Zhuang, N. Lyu, R. Wei, W. Huang, J. Kou and W. Huang, "TokenPool-Scheduler: Token-Level GPU Pooling and Resource Slicing for Multi-Model Co-location."

[12] R. Meng, S. Y. Huang, X. Zhang, Z. Huang, K. Zeng and Y. Yang, "Constraint-Consistent Skill Composition for Reliable Zero-Shot Task Generalization in LLM Agents."

[13] Q. Liu, Y. Zhang, S. Chen, Z. Liu, Y. Xu and H. Cui, "Uncertainty-Aware Marketing Attribution Inference and Budget Decision-Making with Intelligent Agents," 2026.

[14] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[15] A. Zhu, W. Liu, Z. Li, C. Wen, J. Qiu and Z. Liu, "ArcheScale-Guard: Archetype-Aware Predictive Autoscaling with Uncertainty Quantification for Serverless Computing."

[16] X. Yang, S. Li, K. Wu, Z. Wang, Y. Tang and Y. Li, "Adaptive Anomaly Detection in Microservice Systems via Meta-Learning," 2026.

[17] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292-2330, 2008.

[18] R. Ying, J. Lyu, J. Li, C. Nie and C. Chiang, "Dynamic Portfolio Optimization with Data-Aware Multi-Agent Reinforcement Learning and Adaptive Risk Control," 2025.

[19] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia and M. Dohler, "Standardized protocol stack for the internet of (important) things," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389-1406, 2012.

[20] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," Computer Networks, vol. 50, no. 7, pp. 877-897, 2006.

[21] R. Ying, Q. Liu, Y. Wang and Y. Xiao, "AI-Based Causal Reasoning over Knowledge Graphs for Data-Driven and Intervention-Oriented Enterprise Performance Analysis," 2025.

[22] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of things for smart cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, 2014.

[23] C. Chen, R. Fang and J. Lai, "Causal representation learning for robust and interpretable audit risk identification in financial systems," Proceedings of the 2025 7th International Conference on Economic Management and Model Engineering (ICEMME 2025), p. 454, Mar. 2026. Springer Nature.

[24] Waskito, K. T., A. Geraldi, A. C. Ichi, G. P. Rahardjo, and I. Al Ghifari, "Design of hydraulic power take-off systems unit parameters for multi-point absorbers wave energy converter," Energy Reports, vol. 11, pp. 115-127, 2024.

[25] J. Huang, J. Zhan, Q. Wang, J. Jia and B. Zhang, "Stable Fault Diagnosis Under Data Imbalance via Self-Supervised Learning in Industrial IoT," 2026.

[26] Ahmad, T., and D. Zhang, "Using the internet of things in smart energy systems and networks," Sustainable Cities and Society, vol. 68, Art. no. 102783, 2021.

[27] Barbosa, A., H. Mubarak, F. Mohammadi, M. J. Sanjari, and M. Saif, "A real-time IoT-based data acquisition and monitoring system for photovoltaic applications," in Proc. 2024 3rd Int. Conf. Power Systems and Electrical Technology (PSET), Aug. 2024, pp. 667-670.

[28] Hasan, M. K., M. M. Ahmed, B. Pandey, H. Gohel, S. Islam, and I. F. Khalid, "Internet of Things-based smart electricity monitoring and control system using usage data," Wireless Communications and Mobile Computing, vol. 2021, Art. no. 6544649, 2021.

[29] Mirani, A. A., A. Awasthi, N. O'Mahony, and J. Walsh, "Industrial IoT-based energy monitoring system: Using data processing at edge," IoT, vol. 5, no. 4, pp. 608-633, 2024.