International Journal of Informatics and Computation (IJICOM)
Vol. 8, No. 1, 2026
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI: 10.35842/ijicom

Developing Prototype of Modbus IoT Gateway for Odoo ERP Integration

Daniel Yosh Apriando[1], Alfred Tenggono[2]

Abstract

Industrial environments increasingly require seamless integration between field-level devices and enterprise management systems to support real-time monitoring and operational decision-making. However, many industrial devices still rely on the Modbus RTU protocol, which limits direct interoperability with modern Enterprise Resource Planning (ERP) platforms. This paper develops a prototype of a Modbus IoT Gateway for Odoo ERP integration to bridge this communication gap. The proposed system utilizes an ESP32 controller as a Modbus master, Node-RED as middleware, and Odoo ERP as the centralized monitoring and management platform. The gateway acquires data from field devices, converts the information into JSON format, and transmits the data securely through a WPA2-protected wireless network for integration with the ERP system. This study implements a fixed 10-second transmission interval to support near real-time data synchronization while maintaining efficient resource utilization. The system continuously monitors Electrical Conductivity (EC), pH values, relay status, and robotic arm conditions. The acquired data are processed by Node-RED and stored in the Odoo database for visualization and analysis. The Odoo dashboard presents operational information through dynamic graphs and status indicators, enabling operators to observe parameter trends, detect abnormal conditions, and respond promptly to potential operational issues. The implementation results demonstrate successful end-to-end integration between Modbus-based industrial devices and the Odoo ERP platform. The proposed architecture provides reliable data acquisition, secure communication, centralized monitoring, and automated operational supervision. The system improves operational visibility and supports faster decision-making through near real-time information delivery. These findings indicate that the proposed Modbus IoT Gateway offers a practical and scalable solution for integrating industrial automation systems with enterprise applications.

Keywords:
Modbus RTU, IoT Gateway, Odoo ERP, Node-RED, Real-Time Monitoring

1. Introduction

The rapid growth of the Industrial Internet of Things (IIoT) drives industries to connect conventional field devices with cloud-based monitoring, analytics, and control platforms. Many industrial environments still rely heavily on legacy communication protocols, particularly Modbus RTU, because of their simplicity, reliability, and widespread adoption in industrial equipment. However, these devices cannot directly communicate with modern Internet services and cloud infrastructures. As a result, organizations require IoT gateways that bridge traditional industrial networks with modern communication protocols. Researchers have increasingly focused on developing gateway architectures that support seamless data exchange between industrial devices and cloud platforms while preserving compatibility with existing infrastructure. This requirement makes IoT gateways a critical component in Industry 4.0 implementation and digital transformation initiatives. [11], [14], [15], [17]

Corresponding Author: Daniel Yosh Apriando, Jakarta International University, Indonesia (daniel22@jiu.ac)
1 Daniel Yosh Apriando, Jakarta International University, Indonesia
2 Alfred Tenggono, Jakarta International University, Indonesia

Modern industrial environments contain heterogeneous devices that operate using different communication standards, including Modbus RTU, Modbus TCP, CAN Bus, MQTT, and various proprietary protocols. This diversity creates interoperability challenges because devices cannot naturally exchange information across different communication layers. Several studies propose protocol conversion and adaptation mechanisms to address this issue. Sun et al. design a cloud-based gateway that enables communication between CAN Bus and Modbus RTU networks, while Shu et al. introduce a Modbus adaptation method that simplifies application-level interaction with Modbus devices. Similarly, recent OSI-based industrial architectures demonstrate how gateways can integrate PLCs, HMIs, Modbus RTU, Modbus TCP, MQTT, and cloud services into a unified communication framework. These findings indicate that protocol interoperability remains one of the most important challenges in industrial IoT deployment. [13], [16], [19]

Many existing gateway implementations focus on enabling communication between Modbus devices and MQTT-based cloud services. MQTT has become one of the most widely adopted messaging protocols in IoT systems because it offers lightweight communication, low bandwidth consumption, and efficient publish-subscribe mechanisms. Researchers develop various Modbus-to-MQTT gateways using low-cost hardware platforms such as Raspberry Pi, ESP32, and embedded Linux systems. These gateways successfully collect sensor data, convert industrial messages into MQTT topics, and transmit information to cloud applications. Although these solutions demonstrate practical feasibility, many implementations primarily emphasize connectivity and data transmission while paying less attention to scalability, latency optimization, and intelligent gateway management. [11], [14], [15], [17], [23]

Cost efficiency and deployment flexibility also play important roles in gateway development. Industrial organizations often seek solutions that minimize implementation costs while maintaining reliable operation. Several studies utilize affordable embedded platforms such as Raspberry Pi and LinkIt Smart 7688 Duo to reduce deployment expenses. Researchers demonstrate that low-cost hardware can effectively support Modbus communication, MQTT messaging, web-based monitoring interfaces, and sensor integration. Open-source technologies such as Docker and Node-RED further simplify gateway deployment and customization. However, low-cost implementations may face resource limitations that affect processing performance, communication efficiency, and scalability when deployed in large industrial environments. [11], [12], [21], [23]

Beyond interoperability and cost considerations, communication performance remains a significant challenge in industrial IoT systems. Traditional Modbus TCP gateways rely on the TCP protocol stack, which introduces additional communication overhead and latency. As industrial applications increasingly demand real-time monitoring and control, researchers investigate alternative communication mechanisms to improve gateway responsiveness. Zhao proposes an Advanced UDP (AUDP) framework that incorporates CRC verification, retransmission strategies, transaction matching, and exponential backoff mechanisms. Experimental results demonstrate lower communication latency and improved reliability compared with conventional Modbus TCP-based gateways. Similarly, studies on Modbus extensions introduce optimized message formats and deterministic acquisition cycles to improve gateway performance. These developments highlight the growing need for efficient communication architectures that support real-time industrial operations. [1], [18]

The expansion of industrial IoT networks also increases cybersecurity risks. Gateways serve as critical entry points between operational technology environments and external networks, making them attractive targets for cyberattacks. Recent studies investigate intrusion detection frameworks, blockchain-based security mechanisms, deep learning approaches, contrastive learning models, and post-quantum cryptographic techniques to strengthen gateway security. Researchers develop advanced detection systems capable

of identifying anomalous network activities while maintaining communication efficiency in resource-constrained environments. The emergence of quantum computing further motivates the development of quantum-resistant authentication protocols to protect industrial communications against future threats. These developments demonstrate that security has become a fundamental requirement in next-generation IoT gateway design. [4], [5], [7], [8]

Recent advances also show a growing trend toward specialized gateway architectures tailored to particular application domains. Researchers design gateways for smart energy management using NB-IoT communication, industrial automation using PLC-based architectures, smart homes using WiFi, BLE, ZigBee, and Modbus integration, and agricultural monitoring using microcontroller-based systems. These application-specific implementations demonstrate that IoT gateways must support diverse communication requirements while maintaining reliable data acquisition and transmission. However, differences in protocol structures, hardware capabilities, and deployment environments continue to create integration challenges. Therefore, gateway architectures must remain flexible, modular, and adaptable to various industrial scenarios. [9], [19], [20], [22]

Although existing studies provide substantial progress in protocol conversion, cloud integration, communication optimization, and cybersecurity, several research gaps remain. Many gateway solutions focus on individual objectives such as protocol interoperability, low-cost deployment, communication efficiency, or security enhancement. Few studies integrate these requirements into a unified framework capable of delivering high performance, secure communication, flexible protocol adaptation, and scalable deployment simultaneously. Furthermore, emerging industrial applications require gateways that support real-time operation, intelligent management, cloud connectivity, and future-proof security mechanisms. Therefore, this study investigates the design and development of an advanced industrial IoT gateway that addresses these challenges by combining efficient protocol integration, optimized communication performance, and robust system architecture for modern Industry 4.0 environments. [1], [11], [12], [13], [14], [16], [18], [23]

2. Related Works

Early studies focused on bridging legacy industrial devices with modern IoT platforms through Modbus-to-MQTT gateways. Sun et al. designed a gateway using Raspberry Pi and RS485 communication modules to connect Modbus RTU devices with MQTT-based cloud services. The gateway successfully enabled protocol conversion and cloud connectivity for industrial applications. Similarly, Silva and Silva developed a low-cost gateway that mapped Modbus RTU messages into MQTT topics and commands. Their implementation demonstrated reliable bidirectional communication between industrial devices and cloud platforms. These studies established the feasibility of Modbus-MQTT integration. However, they primarily emphasized connectivity and did not address communication latency, scalability, or advanced gateway intelligence. [11], [14]

Several researchers investigated software-centric gateway architectures to improve flexibility and deployment efficiency. Chen and Hsu developed an IoT gateway software system using the LinkIt Smart 7688 Duo platform. Their system integrated Modbus TCP and MQTT communication while providing web-based monitoring interfaces. The proposed architecture enabled remote sensor access and simplified industrial device management. Similarly, Chen and Lin implemented a hardware and peripheral gateway system using the same embedded platform and demonstrated reliable sensor data acquisition through MQTT communication. These studies showed that low-cost embedded devices could support industrial IoT applications effectively. However, they focused mainly on implementation feasibility and provided limited discussion on communication optimization and system scalability. [12], [21]

Researchers also explored protocol adaptation techniques to simplify industrial device integration. Shu et al. proposed a novel Modbus adaptation method that converted Modbus slave data into sensing and actuating information at the application layer. The proposed method abstracted protocol-specific details and simplified software development. The gateway enabled bidirectional data conversion while reducing application complexity. The study improved interoperability between industrial sensors and IoT applications. Nevertheless, the work concentrated on protocol abstraction and did not evaluate performance metrics such as throughput, latency, or reliability under large-scale deployment conditions. [16]

Industrial interoperability remained a major research topic because industrial environments often contained heterogeneous communication protocols. Sun et al. designed a cloud-based gateway that enabled communication between CAN Bus and Modbus RTU networks. The gateway used Raspberry Pi hardware and an intelligent data mapping mechanism to exchange information between different industrial networks. Their results demonstrated successful protocol translation and integration. Likewise, Benavides et al. implemented an OSI-based industrial IoT architecture that connected PLCs, HMIs, Modbus RTU devices, MQTT services, and cloud platforms through a protocol gateway. These studies improved interoperability among industrial systems. However, they focused primarily on protocol conversion and did not extensively address communication efficiency or cybersecurity concerns. [13], [19]

Communication performance became increasingly important as industrial applications demanded real-time monitoring and control. Zhao addressed this challenge by proposing an Advanced UDP (AUDP) mechanism for Modbus gateway communication. The study incorporated CRC validation, retransmission strategies, transaction matching, and exponential backoff mechanisms to improve reliability. Experimental results showed lower latency than conventional Modbus TCP gateways while maintaining communication robustness. In another study, Găitan and Zagan enhanced Modbus extension specifications by introducing optimized message structures and deterministic acquisition cycles. Their implementation improved timing predictability and processing efficiency. Although both studies significantly improved communication performance, they focused mainly on protocol-level optimization and did not integrate broader system-level considerations. [1], [18]

Recent studies increasingly addressed cybersecurity challenges in industrial IoT gateways. Kumar proposed HYBRIDNET-GUARD, a deep learning-based framework for detecting protocol attacks within IoT gateway environments. Hussain developed a blockchain-supported intrusion detection architecture for industrial IoT networks. Shahid introduced a post-quantum authentication protocol based on lattice cryptography to strengthen future communication security. Chen further proposed an unsupervised contrastive learning approach for intrusion detection in low-power IoT devices. These studies highlighted the growing importance of security in industrial systems. However, most of them focused exclusively on security mechanisms and did not consider protocol interoperability, gateway architecture, or communication performance simultaneously. [4], [5], [7], [8]

Researchers also developed application-specific gateway solutions for different industrial and commercial environments. Kopják and Szücs proposed an NB-IoT gateway architecture for energy metering systems. Their design supported remote monitoring and efficient energy management through Modbus-enabled devices. Khanchuea and Siripokarpirom designed a multi-protocol gateway for smart home and building automation environments. The gateway supported WiFi, BLE, ZigBee, RS485, and MQTT communication. These studies demonstrated the adaptability of gateway technologies across different domains. However, their architectures targeted specific application

scenarios and provided limited discussion regarding generalized industrial deployment and interoperability challenges. [20], [22]

Open-source and industrial-scale gateway implementations also attracted significant research attention. Nguyen-Hoang and Vo Tan developed an open-source industrial IoT gateway based on Linux, Docker, and Node-RED technologies. The gateway supported multiple industrial protocols, including Siemens S7, Modbus TCP, Modbus RTU, MQTT, and HTTP. Suryawanshi et al. implemented a Modbus gateway for manufacturing environments using ESP32 and MQTT cloud services. Their solution demonstrated the benefits of Industry 4.0 through improved monitoring and connectivity. These studies showed the practicality of flexible and cost-effective gateway architectures. Nevertheless, they still faced challenges related to communication efficiency, integrated security, protocol adaptation, and real-time industrial performance. Therefore, a comprehensive gateway framework that combines interoperability, performance optimization, scalability, and security remains an important research direction. [17], [23].

3. Proposed Method

The integration workflow starts at the field device layer. This layer consists of an EC sensor, a robotic arm, and a relay module. The devices communicate through the Modbus RTU protocol over an RS485 network. An ESP32 controller acts as the Modbus master. It periodically reads sensor data and device status through a UART-to-RS485 converter. The ESP32 then sends the collected data to the edge gateway using Wi-Fi communication.

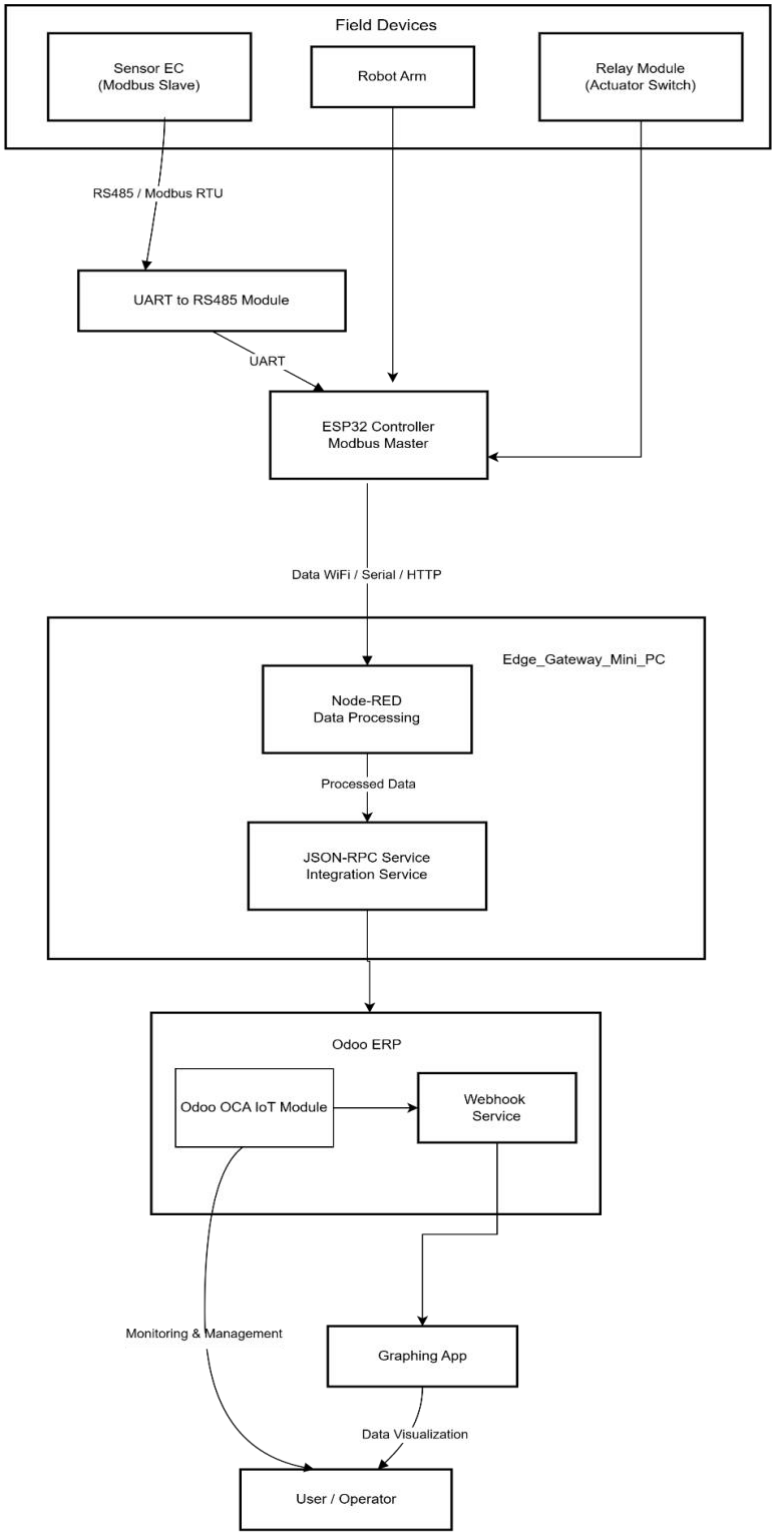


Fig. 1 Workflow Integration

The edge gateway runs on a mini-PC and hosts Node-RED for data processing. Node-RED receives data from the ESP32 and converts it into a structured format. The processed data are forwarded to a JSON-RPC integration service. This service communicates with the Odoo ERP platform through the OCA IoT module and webhook service. Odoo stores and manages the received data for monitoring and operational purposes. A graphical monitoring application retrieves the data from Odoo and displays real-time visualizations to operators. This workflow enables seamless integration between Modbus devices and Odoo ERP for centralized monitoring and management.

In this paper, the proposed Modbus IoT Gateway prototype is evaluated using three key communication performance metrics: latency, throughput, and packet delivery ratio. The latency metric measures the average time required for data to travel from the Modbus device, pass through the IoT gateway, and arrive at the Odoo ERP server. Equation (1) calculates the average latency by determining the time difference between message transmission and message reception across all observed transactions. A lower latency value indicates that the gateway can deliver data more quickly, which is important for real-time monitoring and decision-making applications. This metric allows us to assess the responsiveness of the proposed integration architecture.

1. **Average Latency**

$$L = \frac{1}{N}\sum_{i=1}^{N}(t_{r,i} - t_{s,i}) \quad (1)$$

2. **Throughput**

$$T_p = \frac{D_t}{\Delta t} \quad (2)$$

3. **Packet Delivery Ratio**

$$PDR = \frac{N_r}{N_s} \times 100\% \quad (3)$$

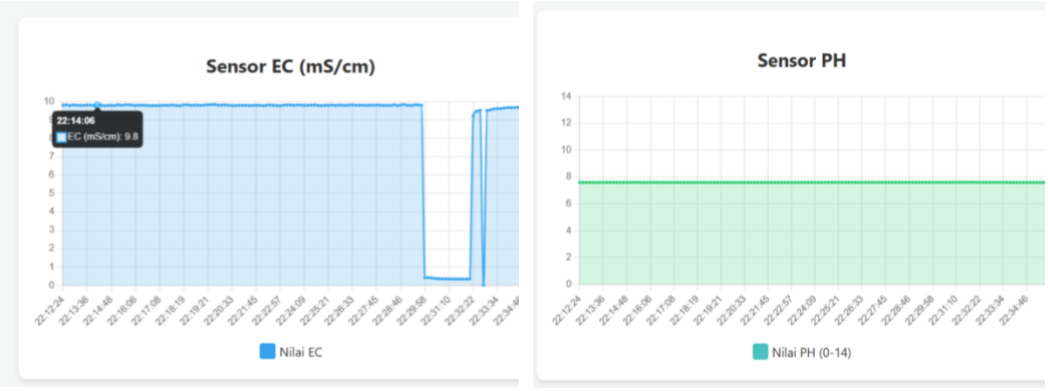
These three metrics are aligned with Modbus IoT Gateway performance evaluation. The throughput metric evaluates the amount of data successfully transmitted from the industrial devices to the Odoo ERP platform within a specific observation period. Equation (2) computes throughput by dividing the total transmitted data volume by the transmission duration. Throughput reflects the communication capacity of the gateway and indicates how efficiently the system handles data traffic generated by Modbus sensors and industrial equipment. A higher throughput value demonstrates that the gateway can process and forward larger volumes of operational data without causing communication bottlenecks.

The Packet Delivery Ratio (PDR) measures communication reliability between the Modbus network and the Odoo ERP server. Equation (3) calculates the percentage of successfully received packets relative to the total number of transmitted packets. A PDR value close to 100% indicates that the gateway reliably delivers data with minimal packet loss. This metric is particularly important in industrial environments because missing data may affect production monitoring, inventory management, maintenance scheduling, and business analytics within the ERP system. Therefore, the combination of latency, throughput, and PDR provides a comprehensive evaluation of the performance, efficiency, and reliability of the proposed Modbus IoT Gateway for Odoo ERP integration.

4. Result and Analysis

The proposed system acquires operational data from field devices through the Modbus RTU protocol and processes the collected information using the Node-RED middleware. After the processing stage, the system forwards the data to the Odoo ERP database for storage, monitoring, and management purposes. This integration enables seamless communication between industrial devices and enterprise applications. The ESP32 controller supports the integration process by providing wireless communication with WPA2 security, which ensures secure data transmission within the local network infrastructure.

To maintain data freshness and support near real-time monitoring, this study configures a fixed transmission interval of 10 seconds. During each cycle, the ESP32 collects sensor readings and device status information, converts the data into JSON format, and transmits the payload to the Node-RED server. Node-RED then processes and forwards the data to the Odoo ERP platform through the integration service. This transmission interval provides a balance between monitoring responsiveness and system resource utilization. As a result, the system continuously monitors water quality parameters, robotic arm conditions, and relay module states without imposing excessive communication or processing overhead on the server. Fig. 2 depicts the End-to-End System Integration Validation.



(a) JSON Payload Transmission Log via HTTP POST

(b) Real-Time Data Visualization

Fig. 2 End-to-End System Integration Validation

The Odoo dashboard visualizes operational data using a rolling 10-minute observation window, with graph updates performed every 10 seconds. This visualization approach enables operators and management personnel to monitor parameter trends and detect abnormal changes in near real-time. For the Electrical Conductivity (EC) parameter, the dashboard presents variations in mineral concentration and salinity levels, which serve as important indicators of process fluid quality. The continuous graphical representation allows users to quickly identify increasing or decreasing trends and respond promptly when measurements approach critical thresholds. Consequently, the dashboard supports faster operational decision-making and enhances the effectiveness of monitoring activities. The EC classification levels used as operational references in the proposed system are presented in Table 1:

Table 1: EC classification levels used as operational references

EC Value Range	Quality Interpretation	Real Field Case Example	Required Action
0.0−1.2 mS/cm	Low / Dilute	Solution lacks mineral content	Add concentrate or nutrients
1.3−2.5 mS/cm	Optimal / Stable	Fluid condition within safe parameters	Routine monitoring on dashboard
>2.5 mS/cm	High / Concentrated	Accumulation of waste or contamination	Partial discharge and dilution

In addition to EC monitoring, the proposed system continuously monitors the pH parameter using the same 10-second transmission interval. The pH value plays an important role in maintaining process stability and preserving the operational lifespan of industrial equipment. Abnormal pH conditions may accelerate corrosion, reduce equipment reliability, and affect overall process performance. By synchronizing pH measurements with the Odoo ERP platform, the system provides centralized and automated supervision of fluid quality. The real-time visualization and historical recording capabilities enable operators to identify deviations promptly and take corrective actions before critical conditions occur. The pH classification levels adopted as operational references in this study are presented in Table 2.

Table 2: pH classification levels adopted as operational references

pH Value Range	Property Interpretation	Operational Risk	Required Action
<6.0	Acidic	Corrosion on metal components	Add alkaline buffer solution
6.0−8.0	Neutral	Ideal condition for most processes	Maintain circulation and filtration
>8.0	Alkaline	Scaling formation on pipes	Normalize temperature or add mild acid

Besides monitoring fluid quality parameters, the proposed system also supervises the operational status of the relay module and robotic arm. The relay status is synchronized with the Odoo ERP platform and displayed as ON or OFF indicators, representing the actual condition of field actuators. In the implemented scenario, the relay controls the circulation and neutralization pumps. When sensor measurements indicate that the pH value falls below the predefined threshold, the system can automatically activate the relay or allow operators to initiate corrective actions through the control interface. Furthermore, the system monitors the robotic arm status at 10-second intervals to ensure that material handling operations are executed according to the scheduled workflow. Continuous monitoring of these devices improves operational visibility, supports timely interventions, and enhances the overall reliability of the industrial process.

5. Conclusion

This paper developed and validated a prototype of a Modbus IoT Gateway for Odoo ERP integration. We utilized the Modbus RTU protocol, an ESP32 controller, Node-RED middleware, and the Odoo ERP platform to establish end-to-end communication between field devices and enterprise applications. The proposed architecture successfully acquired sensor data and device status information, transformed the data into JSON format, and synchronized the information with the Odoo database. The integration process operated reliably through WPA2-secured wireless communication and enabled seamless data exchange across all system components. The findings demonstrate that the proposed gateway effectively bridges industrial devices and ERP systems within a unified monitoring environment.

This study also demonstrated the capability of the proposed system to support near real-time monitoring. We applied a fixed transmission interval of 10 seconds to ensure continuous data acquisition and synchronization while maintaining efficient resource utilization. The Odoo dashboard successfully visualized Electrical Conductivity (EC), pH measurements, relay status, and robotic arm conditions through dynamic graphs and operational indicators. The dashboard allowed operators to observe parameter trends, detect abnormal conditions, and respond promptly when measurements approached predefined thresholds. As a result, the system improved operational visibility and supported faster decision-making based on real-time information.

Furthermore, this paper showed that ERP-based industrial monitoring can extend beyond data collection and provide actionable operational insights. We utilized Odoo as a centralized platform for storing, managing, and visualizing field-level information from multiple devices. The system continuously monitored fluid quality parameters and equipment status while supporting automated and operator-assisted responses through relay control mechanisms. The successful implementation confirms that the proposed Modbus IoT Gateway provides a practical and scalable solution for integrating industrial automation systems with enterprise management platforms. Future work may focus on implementing bidirectional control, predictive maintenance features, and advanced analytics to further enhance Industry 4.0 applications.

References

[1] S. Zhao, “Enhancing Bidirectional Modbus TCP ↔ RTU Gateway Performance: A UDP Mechanism and Markov Chain Approach,” *Sensors*, vol. 25, 2025.

[2] S. Pinjerla, “Multi-stage Decimation with Hybrid CIC-Polyphase Filtering for IoT Gateway Sample Rate Conversion,” *Scientific Reports*, 2026.

[3] J. T., “Enabling IoT Connectivity for ModbusTCP Sensors,” in *Proc. IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA)*, 2020.

[4] K. P. Kumar, “HYBRIDNET-GUARD: An Advanced Deep Learning Framework for IoT Gateway Protocol Attack Detection with MTSS-FE and Wombel Optimization Algorithm (WBOA),” *Journal of Circuits, Systems and Computers*, 2026.

[5] N. Hussain, “Quantum-aware Secure Blockchain Intrusion Detection System for Industrial IoT Networks,” *Scientific Reports*, 2026.

[6] G. Benoit, “FuzzE: Development of a Fuzzing Approach for Odoo's Tours Integration Testing Platform,” in *Proc. IEEE Conf. on Software Testing, Verification and Validation (ICST)*, 2025.

[7] B. Shahid, “Post-quantum Cryptographic Authentication Protocol for Industrial IoT Using Lattice-based Cryptography,” *Scientific Reports*, 2026.

[8] Y. Chen, “CLU-ID: Contrastive Learning Based Unsupervised Intrusion Detection for Low-Power IoT Devices,” *Computer Standards & Interfaces*, 2026.

[9] J. Feng, “Analysis of the Data Processing Method and System Design of the IoT Hardware Gateway Using a Microcontroller,” *Discover Internet of Things*, 2026.

[10] K. Gangaraju, “Energy- and Behavior-aware Sensory Data Collection for ASD Monitoring over IoT Using Unequal Clustering and Reinforcement Learning,” *Discover Internet of Things*, 2026.
[11] C. Sun, K. Guo, Z.-X. Xu, J. Ma, and D. Hu, “Design and Development of Modbus/MQTT Gateway for Industrial IoT Cloud Applications Using Raspberry Pi,” in *Proc. ACM Cloud and Autonomic Computing Conference*, 2019.
[12] Y.-J. Chen and H.-W. Hsu, “Design and Development of IoT Gateway Software System,” in *Proc. Int. Conf. on Computer and Automation Engineering*, 2022.
[13] C. Sun, G. Liu, Z.-X. Xu, D. Hu, and F. Zheng, “Design of Cloud-Based IoT Gateway for CAN Bus to Modbus RTU Integration,” in *Proc. ACM Cloud and Autonomic Computing Conference*, 2022.
[14] C. R. M. Silva and F. A. C. M. Silva, “An IoT Gateway for Modbus and MQTT Integration,” in *Proc. SBMO/MTT-S Int. Microwave and Optoelectronics Conf. (IMOC)*, 2019.
[15] Harjanto, “IoT Gateway Menggunakan Protokol MQTT pada Perangkat Kendali Berbasis Modbus-RTU,” 2020.
[16] F. Shu, H. Lu, and Y. Ding, “Novel Modbus Adaptation Method for IoT Gateway,” in *Proc. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2019.
[17] S. B. Suryawanshi, P. P. Ghadage, N. Chavan, and P. Garade, “IoT Gateway Design and Implementation for Modbus Protocol,” *International Journal of Engineering Applied Sciences and Technology*, vol. 4, no. 2, 2019.
[18] V. Găitan and I. Zagan, “Experimental Implementation and Performance Evaluation of an IoT Access Gateway for the Modbus Extension,” in *Proc. Italian National Conference on Sensors*, 2021.
[19] Benavides, L. Banegas, and L. O. Freire, “IoT Architecture Based on the OSI Model for Industrial Interconnection Using PLC and Modbus Gateway,” *Telecom*, vol. 7, no. 1, 2026.
[20] Kopják and I. Szücs, “NB-IoT Based IoT Gateway Reference Design for Energy Metering,” in *Proc. International Symposium on Applied Computational Intelligence and Informatics*, 2024.
[21] Y.-J. Chen and E.-C. Lin, “Design and Implementation of Hardware and Peripheral System for IoT Gateway,” in *Proc. International Conference on Computing: Theory and Applications*, 2022.
[22] Khanchuea and R. Siripokarpirom, “A Multi-Protocol IoT Gateway and WiFi/BLE Sensor Nodes for Smart Home and Building Automation: Design and Implementation,” in *Proc. 10th International Conference on Information and Communication Technology for Embedded Systems (IC-ICTES)*, 2019.
[23] P. Nguyen-Hoang and P. Vo Tan, “Development an Open-Source Industrial IoT Gateway,” in *Proc. International Symposium on Communications and Information Technologies*, 2019.