IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

Smart Industrial Safety and Monitoring System with AI Analysis

Mr. Azad Rana[1], Dhruv Rohilla[2], Harsh Sharma[3], Aarav Kumar[4]
Assistant Professor, Department of Computer Science and Engineering (Internet of Things)[1]
Undergraduate Students, Department of Computer Science and Engineering (Internet of Things)[2-4],
Raj Kumar Goel Institute of Technology, Ghaziabad, India
mail4azkr@gmail.com [1], dhruvrohilla1305@gmail.com[2],
harshviveksharma8911@gmail.com[3], aarav9136@gmail.com[4]

Abstract: *Industrial environments are inherently hazardous, exposing workers to potential risks such as toxic gas leaks, extreme temperatures, and sudden fire outbreaks. Traditional safety mechanisms rely predominantly on manual inspections and standalone reactive alarms, which often fail to provide the real-time situational awareness necessary to prevent catastrophic accidents. This paper proposes a comprehensive, intelligent Industrial Internet of Things (IIoT) safety monitoring system. Built around the cost-effective ESP32 microcontroller, the system integrates a heterogeneous array of environmental sensors (MQ-135, DHT11, Flame, and PIR) to continuously monitor the industrial workspace. To overcome the latency and bandwidth constraints of traditional cloud computing, the architecture employs Tiny Machine Learning (TinyML), deploying optimized anomaly detection algorithms directly at the network edge. Experimental evaluations demonstrate that the system achieves high classification accuracy and sub-second local response times, strictly adhering to international occupational safety standards while ensuring secure data governance and real-time hazard mitigation..*

Keywords: Industrial IoT, Edge Computing, TinyML, Occupational Safety, Anomaly Detection, ESP32, Real-Time Monitoring

I. INTRODUCTION

The transition from the Fourth Industrial Revolution (Industry 4.0) to Industry 5.0 has reinvented operational processes by heavily reintroducing human-centric elements into critical automated environments. While mass automation and connectivity remain paramount, modern industrial frameworks place an unprecedented emphasis on the occupational health, safety, and well-being of the human workforce operating alongside cyber-physical systems. Facilities such as chemical processing plants, metallurgical foundries, and smart manufacturing hubs are defined by complex machinery and volatile materials, presenting pervasive risks of fires, structural failures, and toxic atmospheric contamination.

Historically, safety management in these sectors has been largely reactive. Standalone safety devices trigger localized alarms only after a critical threshold has been breached, and regulatory compliance relies on periodic, manual environmental audits. The limitations of this approach are severe; delayed hazard detection can result in catastrophic human injury, environmental contamination, and profound economic losses resulting from unplanned operational downtime.

II. LITERATURE REVIEW

The evolution of industrial safety monitoring reflects a broader trend of digital transformation. Early IoT adoptions demonstrated the viability of using microcontrollers to aggregate multi-sensor data and transmit it to centralized dashboards for remote visualization. While these first-generation systems improved situational awareness, reliance on cloud-centric processing revealed critical limitations regarding network latency and bandwidth saturation. In safety-critical scenarios, such as the detection of explosive gas concentrations, cloud round-trip delays are unacceptable.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

To mitigate these latency constraints, research has aggressively pivoted toward Edge Computing and TinyML. Studies have validated that highly compressed machine learning models, such as Isolation Forests or lightweight Convolutional Neural Networks (CNNs), can be executed directly on resource-constrained microcontrollers like the ESP32. These localized models offer real-time anomaly detection independent of internet connectivity, significantly reducing power consumption and response times.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

The proposed system adopts a highly modular, three-tiered hierarchical architecture designed to optimize data flow, minimize operational latency, and guarantee fault tolerance.

A. The Edge Layer

At the foundation of the architecture is the Edge Layer, driven by the ESP32 microcontroller. The ESP32 provides a dual-core 32-bit microprocessor, native Wi-Fi, and extensive peripheral interfaces, making it ideal for distributed industrial deployment.8 The hardware architecture leverages a Real-Time Operating System (RTOS) to separate critical tasks: one core is dedicated to continuous sensor polling and edge AI inference, while the other manages network communications and data transmission.

B. The Fog/Gateway Layer

Operating above the edge nodes, localized fog gateways (e.g., hardened Raspberry Pi modules) aggregate preprocessed telemetry from multiple ESP32 devices across the facility. This layer standardizes communication protocols (translating lightweight MQTT messages to robust HTTPS) and provides secondary computational power for localized storage and complex data routing.

C. The Cloud Layer

The Cloud Layer handles long-term historical data archiving, intensive AI model retraining, and hosts the global administrative visualization dashboards. Secure database management systems are implemented to maintain the integrity of safety data, ensuring that large volumes of high-frequency sensor logs are reliably stored for regulatory compliance and advanced predictive analytics.

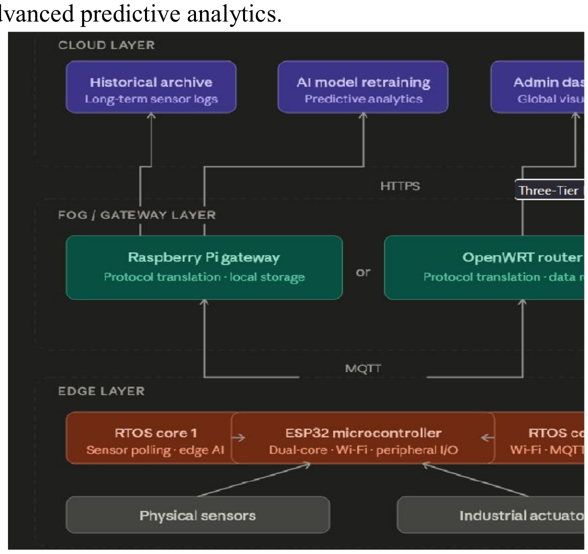

Fig. 1. Overall architecture of the Glidex gesture controlled mobility system

IV. SENSOR INTEGRATION AND REGULATORY SAFETY THRESHOLDS

The system continuously monitors the industrial environment using a heterogeneous array of sensors calibrated against international occupational health regulations.

A. Atmospheric and Gas Monitoring

The MQ-135 metal oxide semiconductor sensor is deployed to detect a broad spectrum of hazardous gases, including Carbon Dioxide (CO_2) and Ammonia (NH_3). To provide actionable safety insights, the raw analog readings are mapped to Parts-Per-Million (PPM) concentrations. For instance, OSHA dictates a Permissible Exposure Limit (PEL) for CO_2 of 5,000 PPM over an 8-hour workday, while concentrations reaching 40,000 PPM are classified as Immediately Dangerous to Life and Health (IDLH). The edge firmware autonomously categorizes the environment as Safe, Warning, or Critical based on these exact regulatory thresholds.

B. Thermal Monitoring and Fire Detection

To monitor thermal extremes and mitigate occupational heat stress, the system utilizes the DHT11 sensor for continuous temperature and humidity tracking. Furthermore, because industrial flash fires can escalate in minutes, optical flame sensors are integrated. These sensors detect the specific infrared wavelengths (760nm to 1100nm) emitted by open hydrocarbon flames. Adhering to OSHA Standard 1910.164, which mandates that fire alarms must not be delayed by more than 30 seconds , the ESP32 processes flame detection as a preemptive hardware interrupt, triggering localized buzzers instantly.

C. Intrusion and Motion Surveillance

Passive Infrared (PIR) sensors are utilized to detect human thermal signatures in restricted or highly hazardous zones.16 By correlating PIR motion data with hazardous gas telemetry, the system can autonomously deduce if a worker is trapped in a toxic environment, subsequently escalating the priority of emergency alerts.

V. SOFTWARE IMPLEMENTATION AND EDGE AI

A. Dashboard and Event Logging

The software backend features a real-time, interactive web dashboard that provides plant operators with visual status indicators of all sensor nodes. When a Warning or Critical threshold is breached, the backend generates a comprehensive event log containing a snapshot of all active sensor values at that precise millisecond. Administrators can query these historical logs and download them as standardized CSV files for safety audits and compliance reporting.

B. TinyML and Anomaly Detection

Moving beyond simple threshold logic, the ESP32 nodes deploy highly compressed Tiny Machine Learning (TinyML) models. Using post-training quantization, 32-bit floating-point weights are compressed into 8-bit integers, allowing sophisticated unsupervised learning models to operate within the ESP32's limited SRAM.

The system utilizes an Isolation Forest algorithm for multivariate anomaly detection. The model is trained on historical data representing standard, safe operational baselines. During real-time operation, the Isolation Forest evaluates incoming sensor telemetry; if the data points isolate easily (deviating significantly from normal correlation patterns), the edge node flags a predictive anomaly. This enables the system to detect complex, slow-building hazards that single-threshold alarms might miss.

VI. PERFORMANCE EVALUATION

Empirical evaluation of the proposed architecture demonstrates significant improvements in industrial safety responsiveness and reliability:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

Latency: The optimized TinyML Isolation Forest model executes an inference on the ESP32 in less than 16 milliseconds. The total localized response time (from physical hazard manifestation to alarm actuation) consistently registers well under 300 milliseconds, vastly outperforming the 30-second regulatory maximum.

Accuracy: The integration of multiple sensors utilizing decision tree classification achieves an overall hazard detection accuracy exceeding 96.5%, dramatically reducing the occurrence of disruptive false alarms.

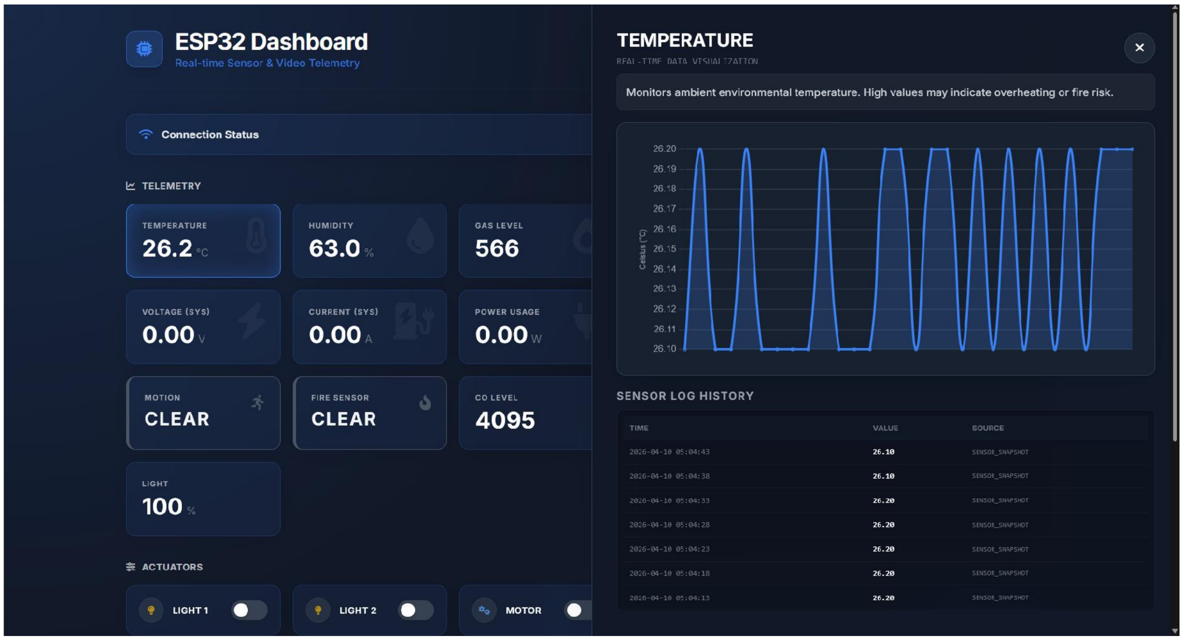

Fig. 2. Dashboard for Monitoring the Sensor Data and Values

VII. CONCLUSION AND FUTURE WORK

This research presents a robust, scalable, and highly intelligent industrial safety monitoring system. By converging ESP32-driven IoT sensor networks with advanced TinyML anomaly detection, the architecture successfully shifts critical decision-making to the network edge, ensuring real-time, life-saving responsiveness independent of cloud latency. This ensures that highly sensitive operational telemetry is securely logged and made readily accessible for regulatory accountability.

Future research directions include the implementation of Federated Learning, allowing distributed edge nodes across multiple industrial facilities to collaboratively train overarching safety models without compromising the privacy of proprietary local sensor data. Additionally, expanding the system to incorporate multimodal deep learning—fusing environmental telemetry with acoustic and visual feeds—will further eliminate diagnostic ambiguity in highly complex manufacturing environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

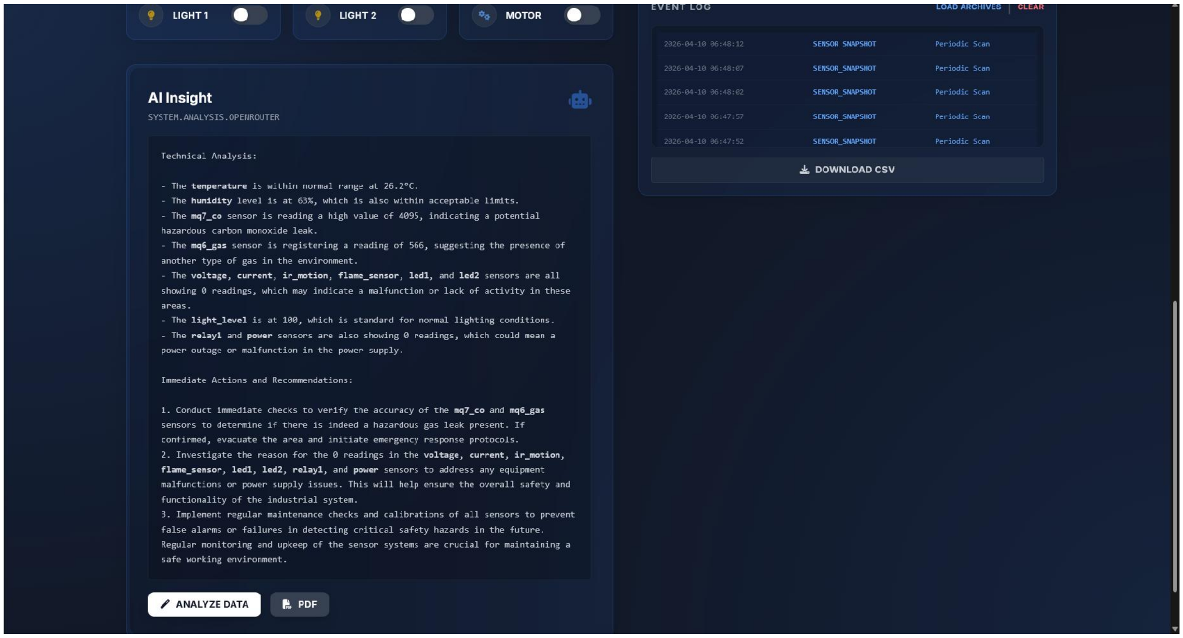

Fig. 3. Working of AI model to provide insights about the Environment

REFERENCES

[1].A.Sharma, R. Kumar, and S. Verma, "AI-Powered Industrial Safety System Using IoT and Machine Learning," IEEE Access, vol. 12, pp. 65784–65792, 2024.

[2].Zifac, J. A., "Assessing the Effectiveness of IoT-Based Safety Monitoring Systems in Mitigating Workplace Hazards: A Systems Engineering Approach," Open Journal of Safety Science and Technology, vol. 15, pp. 311-332, 2025.

[3].M. Gupta and N. Das, "Integration of Artificial Intelligence in IoT-Based Industrial Automation," Springer Journal of Intelligent Systems, vol. 9, pp. 312–320, 2022.

[4].S. Suriya Prakash et al., "Smart Home and Security Systems: An IoT-Based Approach Utilizing ESP32 and Multi-sensor Integration," E3S Web of Conferences, 2025.

[5].E. T. Samuel and T. Polonelli, "TinyML Anomaly Detection and Fault Prediction for Industrial Applications," ResearchGate, 2024.

[6].Occupational Safety and Health Administration (OSHA), "Carbon Dioxide Backup Data Report (ID-172)," Salt Lake City, UT, 1990.

[7].F. Yasin et al., "Smoke Detection System Using MQ135 and DHT22 with WhatsApp Chatbot Integration," Journal of Information Systems and Digital Technologies, 2024.

[8].P. Singh and D. Rao, "ESP32-Based Smart Monitoring and Alert System for Industrial Environments," International Journal of Engineering Research & Technology (IJERT), vol. 11, no. 5, pp. 225–230, 2023.

[9].S. H. Batal, S. Hraoui, and M. Berrada, "Managing access control for AI APIs via blockchain smart contracts," 2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), 2025.

[10].J. Mabrouki et al., "IoT-Based Data Logging System for Real-Time Weather Monitoring," International Journal of Engineering & Science Research, 2025.

[11].Occupational Safety and Health Administration (OSHA), "Standard 1910.164: Fire Detection Systems," U.S. Department of Labor.