SRI RAMACHANDRA
INSTITUTE OF HIGHER EDUCATION AND RESEARCH
(Category - I Deemed to be University) Porur, Chennai
SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

IoT-Ready Industrial Safety Layer

CYB23IN301 Internship -III

First Review
Date:16/12/25

Team Members
Navadeep KM
E0223022

Project Guide
Assistant Professor
Mr. S Manoj Kumanran

INTRODUCTION

Need for the technology

- Industrial environments involve hazardous gases, high temperatures, and heavy machinery
- Manual monitoring is slow and prone to human error
- Accidents often occur due to delayed hazard detection
- IoT enables real-time monitoring and faster response
- Centralized monitoring improves operational safety

Applications

- Industrial plants and manufacturing units
- Chemical processing industries
- Oil refineries and gas pipelines
- Smart industrial safety systems
- Hazardous material storage facilities

INTRODUCTION(continuation)

Challenges to be addressed

- Handling real-time data from multiple sensors
- Filtering noisy or faulty sensor readings
- Avoiding false alerts while ensuring safety
- Designing a scalable backend system
- Ensuring system reliability in critical conditions

Motivation behind the study

- Increasing number of industrial accidents worldwide
- Inefficiency of manual inspection systems
- Need for automated, real-time hazard detection
- Requirement for scalable safety infrastructure
- Growing adoption of IoT in industrial environments

REVIEW OF LITERATURE

Author and Year (chronological order)	Methodology/ Materials and Methods	Datasets	Results/Outcome	Advantage / Key findings from the work	Disadvantage/ GAP Identified from the work
Kumar et al., 2020	IoT-based industrial safety monitoring	Rule-based threshold detection	Early detection of hazardous conditions	Lacks scalable backend pipeline	Kumar et al., 2020
Boyes et al., 2020	Safety & security in Industrial IoT	Risk and threat analysis	Identified IIoT safety risks	No real-time alert implementation	Boyes et al., 2020
Minerva et al., 2020	IoT reference architectures	Layered system design	Standardized IoT architecture	No validation or alert layer	Minerva et al., 2020
Lee et al., 2021	Digital twins for industrial safety	Predictive monitoring	Improved safety prediction	High deployment complexity	Lee et al., 2021
Kumar & Singh, 2021	IoT alert generation systems	Rule-based alert logic	Accurate threshold alerts	Static rules, no adaptability	Kumar & Singh, 2021

REVIEW OF LITERATURE

Author and Year (chronological order)	Methodology/ Materials and Methods	Datasets	Results/Outcome	Advantage / Key findings from the work	Disadvantage/ GAP Identified from the work
Chen et al., 2022	Edge computing for IoT safety	Edge-based data processing	Reduced latency	Limited analytics capability	Chen et al., 2022
Sharma et al., 2022	Cloud-based IIoT platforms	Centralized cloud monitoring	Scalable monitoring	Internet dependency	Sharma et al., 2022
Patel et al., 2023	Hybrid IoT safety frameworks	Edge–cloud integration	Improved reliability	Increased system complexity	Patel et al., 2023
Verma et al., 2023	ML-based anomaly detection	Machine learning models	Adaptive hazard detection	High computation cost	Verma et al., 2023
Rao et al., 2024	Scalable IoT safety pipelines	Microservices architecture	Efficient multi-sensor handling	Limited real-world validation	Rao et al., 2024

REVIEW OF EXISTING SYSTEM

Author /Developer Year (chronological order)	Methodology/ Materials and Methods	Datasets	Results/Outcome	Advantage / Key findings from the work	Disadvantage/ GAP Identified from the work
Manual IoT dashboards (2020)	Basic IoT sensors + cloud	Remote monitoring	No automated alerts	Manual IoT dashboards (2020)	Basic IoT sensors + cloud
Rule-based safety alarms (2021)	Threshold logic	Simple & fast	Static rules	Rule-based safety alarms (2021)	Threshold logic
Cloud-only safety systems (2021)	AWS / Azure IoT	Scalability	Latency issues	Cloud-only safety systems (2021)	AWS / Azure IoT
Edge-based safety systems (2022)	Edge computing	Low latency	Limited analytics	Edge-based safety systems (2022)	Edge computing
Hybrid IoT safety platforms (2023)	Edge + Cloud	Balanced performance	High complexity	Hybrid IoT safety platforms (2023)	Edge + Cloud

PROBLEM STATEMENT

Industrial environments rely on multiple sensors to monitor safety-critical parameters such as gas concentration and temperature. However, existing systems lack a centralized and scalable mechanism to validate multi-sensor data and generate real-time safety alerts. This leads to delayed hazard detection and increased risk of industrial accidents. Hence, there is a need to design a reliable IoT-based safety data pipeline that supports real-time data ingestion, validation, and event-based alert generation.

OBJECTIVES

Objective- 1

- To design a centralized IoT data pipeline capable of ingesting real-time data from multiple industrial sensors.

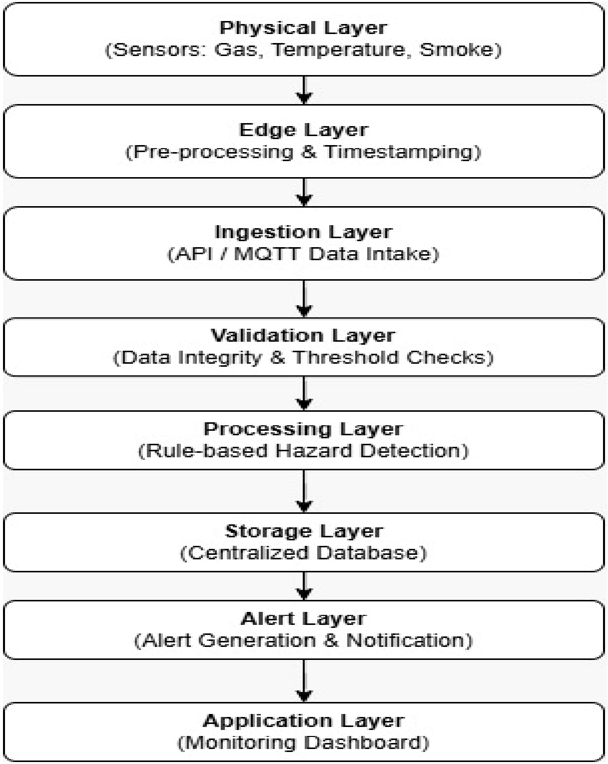
Objective- 2

- To implement a data validation and rule-based event detection mechanism for identifying unsafe industrial conditions.

Objective- 3

- To generate real-time safety alerts and provide a scalable framework that supports future sensor and analytics integration.

WORKFLOWDIAGRAM



MODULES

No.	Modules	Methodology/ Algorithm	Technologies (H/W and S/W)	Implementation
1	Sensor Data Simulation	Simulated sensor value generation	Python	Generates temperature and gas sensor inputs
2	Data Ingestion Module	REST-based data ingestion	FastAPI, Python	Receives sensor data through APIs
3	Data Validation Module	Threshold-based validation	Python	Filters invalid and abnormal sensor values
4	Alert Generation Module	Rule-based alert logic	Python	Generates alerts for unsafe conditions
5	Data Storage Module	Relational data storage	SQLite, SQLAlchemy	Stores sensor data and alert logs

TENTATIVE RESULTS/ EXPECTED OUTCOME

- The proposed system is expected to successfully ingest data from multiple industrial sensors in real time through a centralized backend infrastructure. Sensor readings such as temperature and gas concentration will be validated to ensure data accuracy and reliability before further processing.
- The system is expected to detect unsafe operating conditions by continuously comparing validated sensor data against predefined safety thresholds. When abnormal conditions are identified, real-time alerts will be generated to notify operators and enable quick response, thereby reducing the risk of industrial accidents.
- In addition, the centralized storage of sensor data and alert logs will allow continuous monitoring and future analysis of safety trends. The modular and scalable architecture of the system is expected to support the integration of additional sensors, alert rules, and analytics components in future phases of the project. Overall, the proposed solution aims to improve industrial safety, reduce response time to hazards, and provide a reliable foundation for advanced industrial IoT safety systems.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, “Internet of Things in industries: A survey,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[2] 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, Fourth Quarter 2015.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sept. 2013.

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, no. 1, pp. 146–164, Jan. 2015.

[5] M. Aazam and E.-N. Huh, “Fog computing and smart gateway based communication for cloud of things,” *Future Generation Computer Systems*, vol. 97, no. 1, pp. 628–639, Aug. 2019.

[6] P. P. Ray, “A survey on Internet of Things architectures,” *Journal of King Saud University – Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, July 2018.

[7] K. Ashton, “That ‘Internet of Things’ thing,” *RFID Journal*, vol. 22, no. 7, pp. 97–114, June 2009.

[8] M. Chiang and T. Zhang, “Fog and IoT: An overview of research opportunities,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[9] 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, Feb. 2014.

[10] Y. Chen, S. Deng, H. Ma, and J. Yin, “Deploying data-intensive applications with multiple services on edge,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2169–2182, June 2018.

Thank you