



A Systematic Review of IoT, Machine Learning, and Edge Computing for Real-Time Industrial Hazard Detection

Ashwini Vinod Waghale¹, Dr. K. P. Yadav², Dr. Salim A. Chavan³

¹Research Scholar, Department of Electronics and Communication Engineering, Mats University, Raipur (C.G), India.

²Professor, Department of Computer Science Engineering, Mats University, Raipur (C.G), India.

³Professor, Department of Electronics Engineering, Govindrao Wanjari College of Engineering and

Abstract- There are several types of threats to human safety and industry that include gas leakage, excess temperature, vibration, fire, and machinery malfunction. This literature review aims at assessing the role of Internet of Things (IoT), Machine Learning (ML), and Edge Computing techniques in real-time industrial threat detection and monitoring. The literature review evaluates the use of multi-sensor system, machine learning for classification, Raspberry Pi based edge computing, MQTT communication protocol, and web-based monitoring systems. This paper focuses on Random Forest based classification of hazards, real-time monitoring of sensors, AES-256 Encryption-Decryption, authentication, secure MQTT communication, Flask dashboard, alert generation and relay based machine shutdown techniques. This paper discusses some of the challenges that include lack of real time validation, use of static data, sensor variations, secure data transfer, and combination of intelligent predictions with safety response mechanism. There is scope for future research in areas of secure IoT communication, edge based machine learning, real-time data processing, encryption and industrial safety response mechanism.

Keywords- Industrial IoT, Machine Learning, Random Forest, Edge Computing, Industrial Hazard Detection, Real-Time Monitoring, AES-256 Encryption, MQTT, Raspberry Pi, Industrial Safety.

I. INTRODUCTION

Industrial setups experience several threats ranging from gas leaks, extreme temperature, abnormal vibrations, fires, and failure of the machinery among others. IoT allows constant monitoring using sensors while ML can be used for intelligent detection of any hazard [1]–[4]. Edge computing has also been considered in recent research for processing the data from industrial IoT closer to the origin and avoiding reliance on cloud processing [5], [6]. Despite that, the current approaches face several problems including insufficient real-time validation, dependency on static data, poor multi-sensor fusion capabilities, and security issues [1], [3]. It is crucial, therefore, to have secure communications involving authentication, encryption, and MQTT along with dashboards and alerts for reliable IIoT systems [3], [6].

Data from multi-sensors used together with ML classification may offer a more thorough evaluation of industrial environments than single parameter monitoring. The use of edge computing tools like Raspberry Pi to analyze data and predict risks locally will make risk detection faster and minimize communication latency. Secure data management using encryption and decryption, authentication, and



secured communication using AES may improve data security and integrity in industrial monitoring systems.

This paper reviews past literature on IoT, Machine Learning, Edge Computing, multi-sensor monitoring, secure communication, and automated industrial safety systems. The review will compare current systems, identify the research gaps in each area, and suggest future developments in creating intelligent industrial monitoring systems.

II. RELATED WORK

Chevtchenko et al. [1] performed systematic mapping on the subject of anomaly detection in industrial machines based on the use of IoT devices along with Machine Learning methods. This paper examined 84 scientific papers that were released from 2016 to 2023 and involved popular ML algorithms, data pre-processing methods, and sensors. It demonstrates the increasing significance of data-based methods in industrial anomaly detection and proves that IoT-based sensor data can be efficiently used in order to identify abnormal machine behavior. Nevertheless, it was also stated that there is a need for additional research in the field.

Miorandi et al. [2] gave a detailed review of IoT technologies, applications, and research challenges. This study focuses on the need for distributed sensing, communication, connectivity, and interconnectedness in order to build intelligent IoT applications. The study gives a basic understanding of the way that connected devices can be used to gather and exchange data in order to provide monitoring and decision making. This concept is more applicable to industries where monitoring using sensors is needed all the time. Khan et al. [3] focused on the architecture, applications, and challenges of the Internet of Things. This paper focuses on the need for connectivity and machine-to-machine communications in order to enable communication among devices without human intervention all the time. This paper provides the architectural basis of IoT based monitoring systems and how interconnected devices are useful for gathering real-time data and communicating among each other. However, the increasing number of connected devices brings challenges as well.

In their study, Ni and Li [4] explored ML-assisted security in the Industrial IoT and evaluated the implementation of ML approaches to perform anomaly detection, threat identification, behavior authentication, and incident response. This research reveals the fact that the more connected IIoT system is, the more vulnerable it becomes to cybersecurity threats. Hence, secure communication and intelligent security systems are required to ensure safety and reliability of the operations. It becomes clear that it is crucial to combine security systems with intelligent industrial monitoring.

An IoT-based real-time fire detection system based on Raspberry Pi and fisheye camera was designed by Lee et al. [5]. The system is capable of capturing images and sending them to Firebase via Wi-Fi. Image processing and analysis are performed in order to detect the fire and pinpoint the location of the fire. The paper shows that it is possible to use Raspberry Pi as an affordable computer platform for real-time monitoring of industrial and environmental parameters. Nevertheless, the main emphasis is not put on multi-parameter fire detection and identification.

The use of Raspberry Pi and sensor nodes for industrial hazard prevention was studied by Das et al. [6]. This study highlights the capability of Raspberry Pi based systems in collecting sensor data and providing assistance in industrial hazard prevention. The study is especially relevant to edge-based industrial safety as it shows that an inexpensive embedded computing system can be employed in monitoring industrial settings. Nevertheless, a more advanced implementation of ML classification and secure communication would enhance the capabilities of such systems.



In summary, the current literature is quite impressive in terms of advancements made in IoT for industrial monitoring, Machine Learning based anomaly detection, edge processing using Raspberry Pi, and IIoT Security [1]–[6]. Nevertheless, current research work mainly focuses on specific areas like anomaly detection, fire detection, architecture of IIoT, or cybersecurity. There is room for research in designing a comprehensive industrial safety system that includes multiple sensors for monitoring, edge computing-based ML classification, data encryption for communication, secure MQTT communication, dashboard for live display of data, and automatic response for emergency situations.

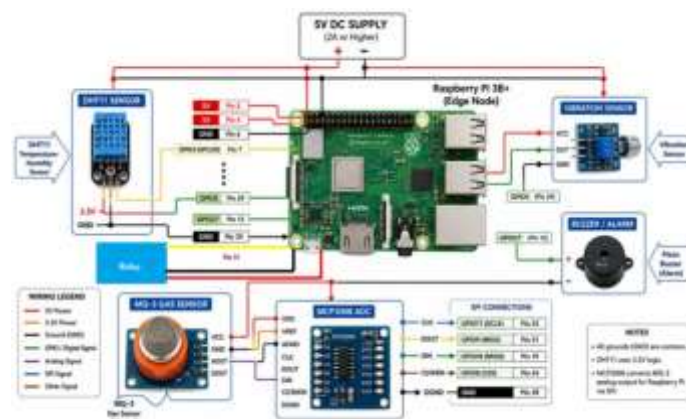


Figure 1: Proposed System

Figure 1: The suggested system is an integrated IoT, Machine Learning, Edge Computing, and security system that detects real-time industrial hazards. Multiple sensors gather data in terms of temperature, humidity, gas, and vibration in real-time from the industrial environment. The gathered data are then sent to the Raspberry Pi 3 Model B+ where the data will undergo preprocessing and Random Forest hazard classification. The industrial environment is classified either safe, normal, moderate, or hazardous through the use of this system. The suggested framework utilizes authentication, data encryption and decryption, and secure MQTT protocol in order to ensure the safety of the transmitted and stored sensor information. The sensor data and their hazard classification are visualized in real-time using a dashboard created by the use of Flask technology. The system triggers a piezo buzzer to warn the workers if a hazardous situation occurs, and it also turns off the machine by switching off its relay module.

A. Challenges and Limitations

Although there is much improvement in the IoT- and ML-driven industrial safety system, there still exist a number of problems. The current solutions usually lack proper validation in practice as they heavily depend on static or benchmarked datasets, making it hard to understand how well the models work in the changing environment. The multi-sensor systems may be impacted by the noises and changes in data that might influence the reliability of the prediction. It is also important to consider the constraints of the edge devices in terms of computational abilities, memory capacity, and response time. Besides, security is an important factor due to the exposure of the sensor data during the communication process, and it needs to be authenticated, encrypted/decrypted, and communicated. Furthermore, the present solutions lack any capability to provide real-time dashboarding and alerts and do not feature any automated actions such as shutdown of the machinery if there is any risk involved.

III. INTERPRETATION

The abovementioned works demonstrate the efficacy of using IoT, machine learning, and edge computing in terms of enhancing the efficiency of monitoring hazards in real-time in industry. The use of IoT makes it possible to obtain the information about the environment in real-time, while machine learning algorithms will help in detecting anomalies and hazardous situations. In addition, edge



computing, particularly when implemented in Raspberry Pi devices, will make it possible to reduce processing time and make local decisions. Nevertheless, the literature review has revealed certain limitations of the technologies, such as lack of real-time verification, inability to integrate multi-sensors, security problems, and absence of automatic emergency response. The combination of Random Forest-based edge classification, encryption/decryption, secure MQTT protocol, real-time dashboards, and notifications is critical in the field of industrial safety.

Table I: Models and Their Description

Sr. No.	Model	Description
1	Random Forest	Combining more than one decision tree to classify industrial conditions like Safe, Normal, Moderate, and Hazardous.
2	Decision Tree	A classification algorithm using sensor parameters and feature conditions for making decisions.
3	Support Vector Machine (SVM)	Algorithms that can separate hazard classes into different sets through decision boundary optimization.
4	XGBoost	Gradient boosting algorithm using sequential decision tree construction to enhance classification.
5	CNN	Algorithm that uses deep learning models and is primarily used for image-based hazard detection in industries like fire, smoke, and equipment-vision detection.
6	LSTM	Recurrent neural network algorithm capable of handling time series sensor data analysis.
7	K-Nearest Neighbors (KNN)	Algorithm that determines the condition of data sample based on class of similar sensor data samples.

IV. FINDINGS

From the review of the existing literature, it is clear that the use of IoT and Machine Learning techniques provides an effective solution to the problem of continuous monitoring and identification of anomalies [1], [4]. A multisensor system may provide a more complete picture of the condition of industries, whereas Edge Computing ensures fast processing and real-time decisions [5], [6]. In addition, security mechanisms like authentication and encryption have gained significance as means of securing Industrial IoT data [4]. Nevertheless, there are several areas where there is a lack of development, including real-time validation, multi-sensor fusion, secure end-to-end communication, and automated alerting.

V. FUTURE ENHANCEMENT

The development of the proposed safety framework in the future would be through refining of sensor accuracy, real-time sensor monitoring, and enhancement of edge based machine learning performance. It would be possible for the framework to be enhanced to include more industrial sensors and larger real-time datasets for classification of hazards under different environmental settings. In the future, the development of the proposed framework would also be towards incorporating AES-256 encryption and decryption methods, MQTT secured transmissions, authentication, historical analysis on the cloud, mobile alerts, prediction maintenance and emergency responses. There would also be optimization of machine learning models for execution of the models on the edge on Raspberry Pi devices in order to



minimize dependency on communication and improve processing time. Other future developments of the framework include logging, trend analysis, early warning system, remote machine control and dashboarding among others.

Objectives

- Designing a system that would perform real-time hazard monitoring in industries by making use of DHT11, MQ-3 gas, and vibration sensors for constant monitoring of the industrial environment.
- Building a hazard classification model using Random Forest algorithm to classify hazards in industrial environments into Safe, Normal, Moderate, and Hazardous categories.
- Deploying the developed Machine Learning model in Raspberry Pi 3 Model B+ to make use of edge-based computation and reduced dependency on cloud computation.
- Securing data gathered from the industrial sensors with the help of authentication, AES-256 encryption/decryption and MQTT-based secure communication.
- Performing real-time monitoring and automatic responses for emergencies through an automated dashboard, piezo buzzer, and relay-based machine shutdown using Flask framework.

Project Overview

The design of the proposed system is that of a Real Time Industrial Hazard Detection and Monitoring System that consists of IoT, Machine Learning, Edge Computing, and Secure Communication Technologies. The system makes use of DHT11, MQ-3 gas and vibration sensors in order to continuously monitor the industrial environment. These sensor values are processed using the Raspberry Pi 3 Model B+ and the trained Random Forest algorithm determines whether the industrial environment is classified as safe, normal, moderate or hazardous. In order to ensure security in the entire process of data collection and processing, the system employs authentication, AES-256 encryption and decryption, and secure communication using the MQTT protocol. A Flask dashboard monitors real-time sensor values as well as the status of hazard detection and gives audio alerts when a hazardous situation is identified and shuts down machines automatically.

TABLE II. OVERVIEW OF ISSUES APPROACHES, METHODS

Sr. No.	Author(s) [Ref]	Issue Discussed	Approach & Method
1	S. F. Chevtchenko <i>et al.</i> [1]	Industrial machinery anomaly detection and the difficulty of identifying abnormal conditions from large IoT-generated datasets.	Systematic mapping of 84 studies covering IoT devices, ML algorithms, preprocessing techniques, sensors, and industrial anomaly-detection applications. (arXiv)
2	D. Miorandi <i>et al.</i> [2]	Major IoT applications, architecture, connectivity, scalability, and research challenges.	Comprehensive review of the IoT vision, applications, enabling technologies, and research challenges for connected systems. (ScienceDirect)
3	R. Khan <i>et al.</i> [3]	IoT architecture, possible applications, and communication challenges.	Analysis of the Internet of Things architecture, applications, and important technical challenges associated with connected devices.
4	C. Ni and S. C. Li [4]	Cybersecurity threats and security challenges in Industrial IoT environments.	Comprehensive survey of ML-enabled IIoT security, including anomaly detection, threat identification,



			behavioral authentication, and incident response. (ScienceDirect)
5	C.-H. Lee <i>et al.</i> [5]	Real-time fire detection and monitoring in industrial environments.	Developed an IoT-based fire detection system using Raspberry Pi and a fisheye camera for real-time monitoring and fire-location detection.
6	P. K. Das <i>et al.</i> [6]	Prevention and identification of industrial hazards using low-cost computing platforms.	Proposed a Raspberry Pi and sensor-based industrial hazard prevention system for monitoring industrial conditions.
7	Y. N. Deshvena and R. R. Kulkarni [7]	Real-time hazard detection and early identification of hazards in the workplace	Application of IoT sensors and wearable technology to gather data regarding environment, machinery, and workers. (STM Journals)
8	T. Nguyen-Da, P. Nguyen Thanh, and M. Y. Cho [8]	Real-time anomaly detection in industrial diesel generators.	Developed an AIoT-based CNN-LSTM model for real-time anomaly detection in industrial diesel generators under Industry 4.0 conditions. (Colab)
9	G. P. Tancredi, G. Vignali, and E. Bottani [9]	Detection of abnormal operating conditions in industrial production.	Integrated Digital Twin, Machine Learning, IoT, and Industry 4.0 technologies for anomaly detection in a food-processing plant. (MDPI)
10	H. Benaddi <i>et al.</i> [10]	Anomaly and security detection problems in Industrial IoT networks.	Proposed an anomaly-detection approach using Distributional Reinforcement Learning and Generative Adversarial Networks (GANs). (MDPI)
11	S. Ruiz-Villafranca <i>et al.</i> [11]	Detection of cyber threats in Industrial IoT environments.	Developed a MEC-IIoT intelligent threat detector using machine-learning boosted-tree algorithms for edge-based threat detection. (ScienceDirect)
12	G. P. M. R. Raman, C. M. Ahmed, and A. Mathur [12]	Challenges in applying ML-based intrusion detection to industrial control systems.	Conducted an experimental evaluation of ML-based intrusion detection and analyzed practical challenges and lessons for industrial control systems. (Springer)
13	A. Frankó <i>et al.</i> [13]	Application of ML to improve production quality, safety, and sustainability in IIoT.	Examined Machine Learning methods for IIoT and smart production, focusing on industrial data analysis and intelligent production processes. (MDPI)



14	A. Khanna <i>et al.</i> [14]	Real-time machine condition monitoring and fault prediction.	Proposed a distributed Industrial IoT and cloud/fog framework where sensor data are processed through fog nodes for feature extraction and machine-condition classification. (ScienceDirect)
15	T. Zhukabayeva <i>et al.</i> [15]	Real-time cybersecurity and multiclass attack detection in Industrial IoT.	Integrated Machine Learning, XGBoost, Deep Neural Networks, and Edge Computing for multiclass intrusion detection across multiple datasets. (Sage Journals)

VI. CONCLUSION

This review presents the increasing relevance of IoT, machine learning, and edge computing in creating intelligent systems to monitor hazards in industries. Research works indicate the success of multi-sensors monitoring systems, machine learning anomalies detection, Raspberry Pi edge computing, and secure communication through IIoT. However, problems persist in real-time validation, sensor deployment, security of data, and automation of emergency response. A proposed solution includes an integrated system which involves Random Forests classifier in edge computing, AES-256 encryption/decryption, secure communication through MQTT, real-time dashboard monitoring, and alerting/machine shutdown. In general, the aforementioned technologies lay a good basis for designing secure and intelligent industrial safety systems.

REFERENCES

1. S. F. Chevtchenko et al., "Anomaly detection in industrial machinery using IoT devices and machine learning: A systematic mapping," *IEEE Access*, vol. 11, pp. 128288–128305, 2023, doi: 10.1109/ACCESS.2023.3333242.
2. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.
3. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Frontiers of Information Technology (FIT)*, 2012, pp. 257–260, doi: 10.1109/FIT.2012.53.
4. C. Ni and S. C. Li, "Machine learning enabled Industrial IoT security: Challenges, trends and solutions," *Journal of Industrial Information Integration*, vol. 38, Art. no. 100549, 2024, doi: 10.1016/j.jii.2023.100549.
5. C.-H. Lee, W.-H. Lee, and S.-M. Kim, "Development of IoT-based real-time fire detection system using Raspberry Pi and fisheye camera," *Applied Sciences*, vol. 13, no. 15, Art. no. 8568, 2023, doi: 10.3390/app13158568.
6. P. K. Das et al., "Industrial hazard prevention using Raspberry Pi," in *Intelligent Computing and Smart Communication 2019*, Springer, 2020, pp. 1487–1499, doi: 10.1007/978-981-15-0633-8_146.
7. Y. N. Deshvena and R. R. Kulkarni, "IoT-based industrial safety monitoring system," *Journal of Industrial Safety Engineering*, 2024.
8. T. Nguyen-Da, P. Nguyen Thanh, and M. Y. Cho, "AIoT-based real-time anomaly detection for industrial diesel generators," *Internet of Things*, 2024.
9. G. P. Tancredi, G. Vignali, and E. Bottani, "Digital twin, machine learning and IoT for anomaly detection in an industrial production system," *Sensors*, vol. 22, no. 11, Art. no. 4143, 2022.



10. H. Benaddi et al., "Anomaly detection in industrial IoT networks using distributional reinforcement learning and generative adversarial networks," *Sensors*, vol. 22, no. 21, Art. no. 8085, 2022.
11. S. Ruiz-Villafranca et al., "Intelligent threat detection for industrial IoT using machine learning at the edge," *Computer Networks*, 2023.
12. G. P. M. R. Raman, C. M. Ahmed, and A. Mathur, "Experimental evaluation of machine learning-based intrusion detection for industrial control systems," *Journal of Cyber Security Technology*, 2021.
13. A. Frankó et al., "Machine learning applications for industrial IoT and smart production," *Sensors*, vol. 22, no. 23, Art. no. 9148, 2022.
14. A. Khanna et al., "Industrial IoT-based machine condition monitoring using fog computing and machine learning," 2023.
15. T. Zhukabayeva et al., "Machine learning and edge computing for multiclass intrusion detection in Industrial IoT," *Journal of Advanced Transportation Technologies*, 2025.