Machine Learning- Based Smart Laboratory Safety Monitoring System

A. Chenna kesava Reddy[1*], G. Bhagya Lakshmi[2], O. Bharathi[3], N. Sandhya[4], D. Charishma Indhu[5].

Vignan's Nirula Institute of Technology and Science for Women[2,3,4,5,] Palakaluru Road, Guntur-522009, Andhra Pradesh, India

ABSTRACT: Laboratory safety is a vital concern in research and industrial settings where hazardous materials and equipment are often present. Traditional safety systems usually depend on manual monitoring, which can cause delays in responding to emergencies. The Smart Lab and Safety Monitor solve this problem by using Internet of Things (IoT) sensors and machine learning (ML) algorithms for continuous, real-time monitoring of important environmental factors like temperature, humidity, gas concentration, smoke, fire, and motion. Sensor data are sent to a central processing unit for analysis, allowing the system to identify abnormal conditions and alert users immediately through alarms or notifications. Machine learning models predict potential hazards and evaluate risk levels based on past data trends. This intelligent system improves laboratory safety by reducing human error, speeding up response times, and supporting preventive maintenance. Experimental results show that the proposed system offers reliable monitoring, leading to a safer and more efficient lab environment. The use of IoT and AI-driven analytics marks a significant step forward in creating smart, autonomous, and proactive laboratory safety systems for contemporary scientific research.

Keywords: Monitoring, Gas Leak Detection, Machine Learning, Real-time Monitoring, Smoke and Fire Detection

1. INTRODUCTION

In modern laboratories, safety is very important because of the frequent handling of chemicals, gases, and electrical equipment that can be hazardous [1]. Traditional safety systems rely heavily on manual supervision and human intervention, which can delay responses during emergencies [2] [3]. To address these issues, the Smart Lab and Safety Monitor introduce an automated technology-driven approach to laboratory safety management [4] [5]. By using Internet of Things (IoT) sensors and Machine Learning (ML) algorithms, this system continuously monitors environmental factors such as temperature, humidity [6], smoke, gas leaks [7], and fire [8]. Real-time data from sensors are analyzed to identify abnormal conditions, allowing the system to issue instant alerts through alarms or notifications [9] [10].

The ML component improves prediction accuracy by spotting potential risks before they turn into serious problems [11]. This smart monitoring setup not only creates a safer working environment but also supports efficient resource management and preventive maintenance [12] [13]. The proposed system shows how combining IoT and AI technologies can change traditional laboratories into smart, secure, and flexible environments for scientific research and experimentation [14] [15].

2. LITERATURE SURVEY

Xinqing Xiao (2024) created a smart sensing system that uses capacitive liquid-level sensors, Arduino, and Bluetooth for managing safety in laboratories [16] [17]. This system allows for real-time monitoring, visualization, and tracking of hazardous chemicals [18]. It has benefits such as low cost, easy access to its source code, and better safety efficiency [19]. However, it faces challenges related to calibration accuracy, scalability, and integration with current systems [20]. Hussein et al. (2024) created an IoT-based environmental monitoring system that uses sensors for temperature, gas, flame, and pH. This system employs Arduino and ESP32 microcontrollers to manage lab safety and sustainability in real-time [21] [22]. It identifies hazards such as fire, gas leaks, and high temperatures [23]. When these dangers are detected, it sends automatic alerts and takes action through Telegram notifications [24].

The system is low-cost and provides real-time monitoring and automation, which improves safety [25]. However, it has some drawbacks, including limited scalability, reliance on network connectivity, and issues with sensor calibration accuracy [26]. Deepak Adhav et al. (2019) proposed a smart laboratory automation system that uses IoT with Raspberry Pi and OpenCV for facial recognition-based access, device control, and environmental monitoring [27]. The system automates lights, fans, curtains, and fire detection to reduce human effort and energy consumption while improving lab security [28] [29]. Its advantages include low cost, remote access, and efficient energy use. However, it has limitations, such as a need for continuous power and internet connection [30].

Bragatto et al. (2018)[10] developed Smart Safety Systems (SSS) featuring IoT-based wireless sensors to monitor and supervise essential equipment in hazardous process plants. Safety is improved with real-time corrosion, erosion and vibration detection, which allows for risk management changes on the fly [31]. Enhanced reliability and maintainability is available, but standardisation and system maturity are constrained [32]. Shital B. Gite et al. (2022) suggested a smart lab monitoring system that uses IoT, NodeMCU, and sensors to detect temperature, humidity, and gas levels in real time [33]. It improves safety by sending remote alerts. However, it relies on the internet and is limited by the accuracy of the sensors [34].

Using sensors such as RFID, LDR, DHT11, and IR, Shrutika Narhari et al. (2018) created a Bluetooth-based IoT Lab Automation System that allows lab equipment to be controlled and monitored through an Android app [35] [36]. The system is limited by Bluetooth range and scalability for larger environments, but it offers energy efficiency, remote control, and low-cost automation [37]. Using a Raspberry Pi with PIR, DHT11, and light sensors, Banagar and Khattar (2020) created an Internet of Things-based Smart Laboratory System for automated appliance control [38]. Through real-time monitoring, it improves efficiency and lowers energy consumption [39]. It does, however, face difficulties such as security threats and system complexity. In order to improve efficiency, comfort, and safety, Gavrilov et al. (2020) used ambient intelligence and multi-agent systems to design a smart school laboratory. Its high system complexity and setup difficulty limit its ability to automate monitoring and hazard prevention. Firoz Khan et al. (2021) discussed Cyber-Physical Systems (CPS) connected with IoT for smart cities to improve automation and efficiency in areas like transport and energy [40]. It provides real-time monitoring and sustainability, but it faces challenges with security and implementation. Chetna Bhisekar et al. (2018) created an IoT-based water monitoring system using sensors to measure pH, turbidity, temperature, and flow. This system integrates with Arduino and the Blynk app. It allows for real-time detection of water quality and remote monitoring over the internet. The system is low cost, flexible, and automated, but its effectiveness is limited by sensor accuracy and reliance on network connectivity.

3. PROPOSED METHODOLOGY

The proposed Smart Lab and Safety Monitor combine sensors like DHT11, MQ-series, capacitive, and PIR with Arduino or ESP32 for real-time tracking of conditions. Data is cleaned and analyzed using machine learning algorithms to spot anomalies and predict risks. Alerts are sent through alarms, SMS, or web notifications when conditions are unsafe.[16] The system improves safety by automating processes and detecting issues early, but it relies on network, sensor accuracy, and power reliability.[23]

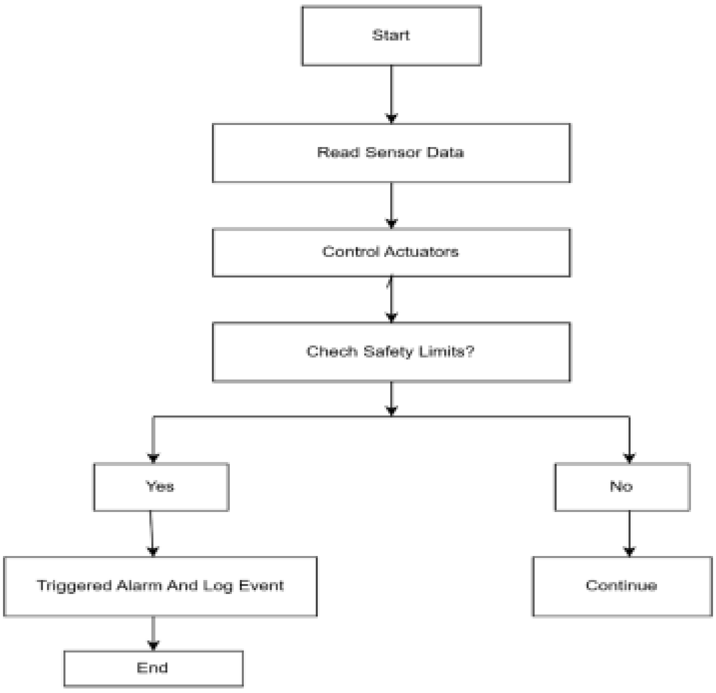

Figure 1: Flowchart of Smart Lab Safety Monitoring System

Algorithm: Smart Lab and Safety Monitor

1. **Input Dataset:**
Collect dataset $D = \{(x_i, y_i)\}_{i=1}^{n}$ containing sensor readings — temperature, humidity, smoke, gas, flame, motion, and time.
2. **Data Cleaning:**
Remove duplicate, irrelevant, and faulty sensor records to ensure data quality.
3. **Anonymization:**
Anonymize and encrypt sensitive data to maintain privacy.
4. **Missing Values Handling:**
Replace missing numeric values with the median and categorical values with the mode.
5. **Outlier Detection:**
Detect outliers using z-score: $|Z_i| = \frac{x_i - \mu}{\sigma} > 3$
6. **Feature Encoding:**
Apply one-hot encoding to categorical features such as time or status indicators.
7. **Normalization:**
Normalise numeric attributes using min-max scaling: $x' = \frac{x - x_{min}}{x_{max} - x_{min}}$
8. **Feature Generation**
Generate derived features such as f=smoke level×temperature or motion count per interval.
9. **Feature Selection:**
Use Recursive Feature Elimination (RFE) to retain the most relevant safety-related features.
10. **Dataset Splitting:**
Split data into training (70%), validation (15%), and testing (15%) sets.
11. **Model Initialisation:**
Initialize Random Forest parameters — n_estimators, max_depth, max_features.

12. **Model Training:**
Train Random Forest using bootstrap samples; compute best splits using Gini impurity or MSE.
13. **Prediction Aggregation:**
Aggregate predictions — majority voting for classification or averaging for regression.
14. **Hyperparameter Tuning & Evaluation:**
Use Grid Search with 5-fold Cross Validation; evaluate Accuracy, Precision, Recall, F1-score, and ROC-AUC.
15. **Feature Importance & Deployment:**
Compute feature importance $I(f_j)$ and deploy the trained model for real-time safety monitoring and alert generation.

4. RESULTS AND ANALYSIS

Figure shows the training performance of the reinforcement learning agent in the smart laboratory safety monitoring environment. The total reward per episode rises quickly during the early training phase, showing that the agent learns effective safety management strategies.[17-18] At first, the agent struggles with inconsistent performance, receiving large negative rewards (between −1000 and −200) due to unsafe or inefficient actions. [22] However, as training continues, the total rewards approach zero, indicating that the agent increasingly performs safe and effective actions. After about 100 episodes, the performance becomes stable, suggesting that the agent has successfully found a reliable policy. This result shows that the RL-based safety monitoring framework can independently learn to reduce risk events and improve operational safety in a smart laboratory setup.[19]

Figure 2: Training rewards over episodes

5. CONCLUSION

The Smart Lab and Safety Monitor system offers an effective and smart way to ensure safety in laboratory settings. It uses sensors to track factors like temperature, humidity, gas leaks, smoke levels, and fire, allowing the system to identify potential dangers in real-time and notify users right away. This active monitoring reduces risks, prevents accidents, and creates a safer work environment for researchers and students. [20-21]By incorporating IoT and machine learning technologies, the system improves automation, reliability, and decision-making based on data. Overall, this system plays a key role in managing laboratory safety by combining smart sensing, constant monitoring, and prompt response strategies. It sets the stage for better and safer smart lab setups in the future.

REFERENCES

[1]. Xiao, Xinqing. "Smart sensing for laboratory safety management." Journal Of Artificial Intelligence 1.1 (2024): 11-16.

[2]. Hussein, Nadia Mahmoud, Yasmin Makki Mohialden, and Saba Abdulbaqi Salman. "Impact of IoT-based environmental monitoring on lab safety and sustainability." Babylonian Journal of Internet of Things 2024 (2024): 16-26.

[3]. Adhav, Deepak, Rahul Pagar, and Ravi Tawade. "Smart Laboratory." International Journal of Trend in Scientific Research and Development 3.3 (2019).

[4]. Bragatto, Paolo, Silvia Maria Ansaldi, and Canio Mennuti. "Improving safety of process plants, through smart systems for critical equipment monitoring." Chemical Engineering 67 (2018).

[5]. Tarakeswara Rao; R. S. M. Lakshmi Patibandla; V. Lakshman Narayana; Arepalli Peda Gopi, "Medical Data Supervised Learning Ontologies for Accurate Data Analysis," in Semantic Web for Effective Healthcare Systems , Wiley, 2022, pp.249-267, doi: 10.1002/9781119764175.ch11.

[6]. C.R.Bharathi, Vejendla. Lakshman Narayana , L.V. Ramesh, (2020),"Secure Data Communication Using Internet of Things", International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.

[7]. Sirisha, A., Chaitanya, K., Krishna, K. V. S. S. R., & Kanumalli, S. S. (2021). Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation. International Journal of Safety and Security Engineering, 11(1), 51-58.

[8]. Kosaraju, Chaitanya, et al. "Mirchi crop yield prediction based on soil and environmental characteristics using modified RNN." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.

[9]. Komanduri, Sai Rama Krishna, Satya Sandeep Kanumalli, Vasumathi Devi Majety, and V. Sujatha. "Malicious Code Detection Using Deep Learning Based LSTM Model." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 2023. https://doi.org/10.1063/5.0137178.

[10]. Sujatha, V., Tejaswi, Y., Pravalika, V., Pavani, P., and Sravani, Ch. "Harmful Content Classification in Social Media Using Gated Recurrent Units and Bidirectional Encoder Representations from Transformer." Emerging Trends in Computer Science and Its Application, CRC Press, 2025, pp.

[11]. Narayana, Vejendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology." Rev. d'Intelligence Artif. 33.1 (2019): 45-48.

[12]. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.

[13]. Lakshman Narayana Vejendla and Bharathi C R, (2018), "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS", Modelling, Measurement and Control A, Vol.91, Issue.2, pp.73-76.

[14]. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., Khadherbhi, R. (2021). Traffic Analysis Using IoT for Improving Secured Communication. In: Reddy, A., Marla, D., Favorskaya, M.N., Satapathy, S.C. (eds) Intelligent Manufacturing and Energy Sustainability. Smart Innovation, Systems and Technologies, vol 213. Springer, Singapore. https://doi.org/10.1007/978-981-33-4443-3_48

[15]. Kumari, G. R. P., Jahnavi, M., Harika, M., Pavani, A., & Lakshmi, C. V. (2023). Smart traffic signal control system using artificial intelligence. In Intelligent Communication Technologies and Virtual Mobile Networks (pp. 829-838). Singapore: Springer Nature Singapore.

[16]. Naresh, A., TSLP, H., Ch, G., & Kumari, G. R. P. (2023, July). Early Prophecy of Low-Birth-Weight Babies Using BM Error Rate Classifier. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[17]. P. S. Krisha and S. R. Peram, "A Brief Survey on Image Denoising based Feature Extraction and Classification Models for Oral Cancer Detection," *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, 2023, pp. 702-708, doi: 10.1109/ICSCDS56580.2023.10104790.

[18]. Rao, S. S., Rao, P. N., Babu, R. M., & Ramakrishna, K. V. S. S. (2024). A GAME THEORETIC COGNITIVE SPECTRUM SENSING SCHEME FOR IoT NETWORKS. Telecommunications and Radio Engineering, 83(9).

[19]. Chaitanya, Prathipati Silpa, et al. "Distracted Driver Detection using Inception V1." 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2023.

[20]. Kavishwar, S. (2011). Pension funds as an infrastructure financing avenue: An exploratory study. *Management Dynamics*, *11*(2), 33-45.

[21]. Bidwaikar, V. N., & Kavishwar, D. S. (2012). Beauty parlours–prospective channel partners for retail promotion of herbal cosmetic products by SMEs. *Indian Streams Research Journal.* 2(1), 1-4

[22]. Shahu, A., Tiwari, H., Joshi, M., & Kavishwar, S. An Analysis of the Effectiveness of Index ETFS and Index Derivatives in Covered Call Strategy. *Journal of Informatics Education and Research.* 4(3), 42-48.

[23]. Jingar, N. K. (2022). Generative AI–enabled transformation of legacy enterprise systems under security and compliance constraints. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 760–770. https://doi.org/10.32628/CSEIT23906219

[24]. Nirmal Kumar Jingar. (2021). Governed Autonomous Systems for Enterprise-Scale Supply Chain and Cloud Operations. In International Journal of Science, Engineering and Technology (Vol. 9, Number 6). Zenodo. https://doi.org/10.5281/zenodo.18629297

[25]. R. Eswarawaka, M. Nijim, V. Kanumuri and H. Albetaineh, "Assessing the Efficacy of Machine Learning and Deep Learning in the Field of Cyber Security," 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA, 2023, pp. 2398-2404, doi: 10.1109/CSCE60160.2023.00388.

[26]. M. Nijim, V. Kanumuri, H. Albetaineh and A. Goyal, "Intelligent Monitoring and Management of Smart Buildings Using Machine Learning: Optimizing User Behavior and Energy Efficiency," 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA, 2023, pp. 2391-2397, doi: 10.1109/CSCE60160.2023.00387.

[27]. Racha, Ganesh. “Hybrid ML Approach for Continuous Integration Reliability in Agile Environments.” United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 3, 2025, pp. 9–21.

[28]. Racha, Ganesh. “Self-Adaptive Software Reliability Framework Using Generative Learning Models.” International Journal for Modern Trends in Science and Technology, vol. 12, no. 1, 2026, pp. 30–37.

[29]. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.

[30]. Veginati, Navya. “Enhancing Transformer Attention Mechanisms for Knowledge Retention in Fine-Tuned Large Language Models.” International Journal of Scientific Research in Science and Technology, vol. 11, no. 5, Sept.–Oct. 2024, pp. 864–871. DOI: https://doi.org/10.32628/IJSRST52310284

[31]. Jonnalagadda, Pawan Kalyan. “AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems.” International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.

[32]. Jonnalagadda, Pawan Kalyan. “Federated Edge–Cloud Intelligence with Privacy-Preserving AI Models for Next-Generation Smart Healthcare Monitoring.” United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 4, Dec. 2025, pp. 46–57.

[33]. Ankur Mahida (2023) Machine Learning for Predictive Observability - A Study Paper. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-252. DOI: doi.org/10.47363/JAICC/2023(2)235

[34]. "Ankur Mahida (2023) Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi.org/10.47363/JMCA/2023(2)135"

[35]. Tummuri, S. S. R. (2024). Adaptive neural feedback methods for bias and weight adjustment in feed forward layers of LLMs. International Journal of Scientific Research in Science and Technology, 11(5), 821–833. https://doi.org/10.32628/IJSRST52310380

[36]. Tummuri, S. S. R. (2023). Quantization aware training techniques for efficient transformer-driven large language models. International Journal of Scientific Research & Engineering Trends, 9(2).

[37]. B. K. Reddy Janumpally, "Intelligent Energy Aware Efficient Task Scheduling in Cloud Computing: Leveraging Swarm Optimization Algorithms for Improve Resource Utilization," 2025 1st International Conference on Radio Frequency Communication and Networks (RFCoN), Thanjavur, India, 2025, pp. 1-6, doi: 10.1109/RFCoN62306.2025.11085278.

[38]. Janumpally, Bharath Kumar Reddy. (2026). Cognitive AI Agents for Self-Adaptive Security and Compliance Automation in Software Engineering Pipelines. 10.1109/ICAUC68182.2026.11441048.

[39]. Kotadiya U, Arora AS, Yachamaneni T. Fintech Innovations in Credit Card Origination: A Multi-Stage Analysis of Algorithmic Lending Models. IJAIDSML [Internet]. 2023 Jun. 30 [cited 2026 Apr. 5];4(2):91-100.

[40]. Arora AS, Yachamaneni T, Kotadiya U. A Comprehensive Analytical Framework for Modeling Consumer Credit Card Behavior and Risk Profiling Using Advanced Financial Metrics. IJAIDSML [Internet]. 2022 Jun. 30 [cited 2026 Apr. 2];3(2):90-100.