JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Biometric Authentication and Risk Alert System for Chemical Laboratories

Atharva Gaikwad
Department of Electronics & Telecommunications
AISSMS Institute of Information Technology
Pune, Maharashtra, India
atharvagaikwad7091@gmail.com

Debshika Dutta
Department of Electronics & Telecommunications
AISSMS Institute of Information Technology
Pune, Maharashtra, India
debshika06dutta@gmail.com

Vaishnavi Ghatge
Department of Electronics & Telecommunications
AISSMS Institute of Information Technology
Pune, Maharashtra, India
vaishnavighatge77@gmail.com

Yash Badade
Department of Electronics & Telecommunications
AISSMS Institute of Information Technology
Pune, Maharashtra, India
yashbadade234@gmail.com

Dr. Shobha Nikam
AISSMS Institute of Information Technology
Pune, Maharashtra, India
Shobha.nikam@aissmsioit.org

***Abstract*—When chemical laboratories are exposed to harmful gases like toluene, they pose significant safety issues, leading to severe health problems. Inadequate gas detection systems and unauthorized access cause serious safety risks. This project aims to improve safety and security of chemical laboratories by combining biometric authentication with real-time gas detection. Biometric authentication system has been widely used in the industries for safety while gas detection system is important for industrial safety. However, both these systems work independently and thus, leaves the gap in providing complete safety solutions. The system uses microcontrollers, fingerprint module for biometric authentication and gas detection sensors for gas detection. Wirelessly, real-time data and risk warnings are transmitted. A model was built consisting of fingerprint authentication system and gas detection system. Entry is controlled by fingerprint authentication system, while the gas detection system inside the lab triggers alarms and locks door if toluene level exceeds 200 ppm.**

***Keywords*—Biometric Authentication, Gas Detection System, Occupational Safety and Health Administration.**

I. INTRODUCTION

The concept of Biometric Authentication has progressed gradually with early applications depending on fingerprint recognition tracing back to the late 19th century. With initial technological breakthroughs, biometrics have been implemented into modern security technologies which assures reliable identity verification. Simultaneously, safety regulations of workplace have become more concerned with gas detection due to the health risks posed by harmful substances like toluene. Toluene is a volatile organic chemical which is used in man industrial processes. It can cause brain damage and other health issues if exposed to toluene for a long time. In Biometric Authentication, biological traits like fingerprints are used to verify identity of a person. Gas Detection system consist of sensors that continuously monitors the quality of air and detects the harmful gases. Occupational Safety and Harmful Administration is a regulatory agency that sets acceptable levels of exposure to dangerous substances at work.

In chemical laboratories, high-level security protocols are required to prevent unverified access and decrease risks involved with harmful substances. Existing access control systems can be compromised as they primarily use passwords or key cards. To add to this, personnel are at risk of hazardous gas exposure as gas detection devices operate independently without an integrated access control mechanism. This research seeks to close this gap by integrating biometric authentication with real-time gas detection that restricts the access based on both identity verification and environmental safety conditions.

The automated, dual-layer security systems have become more important as the laboratory accidents have increased due to exposure to hazardous gases and unauthorized entry in the laboratory. Traditional security systems are not capable of preventing exposure risks as they do not restrict access based on environmental safety. By integrating biometric authentication with gas detection system, it is ensured that laboratory personnel are protected from toxic gas leaks while enforcing strict access control.

The paper "Securing Hardware Accelerators for CE Systems Using Biometric Fingerprinting" [1] is about securing hardware accelerators with biometric fingerprinting but it excludes real-time authentication and environmental monitoring [1]. The research article "Hardware Implementation of Cancellable Biometric Systems" [2] uses cancellable biometrics for security. However, it focuses on biometric encryption and reaction time, the system lacks gas detection and real-time hazard monitoring [2]. The study "Establishing Security Using Cryptography Biometric Authentication" [3] uses encryption-based authentication to increase security. Though it does not cover environmental safety monitoring [3]. The research paper "Survey on Security of Biometric Data Using Cryptography" [4] covers a variety of cryptographic techniques, including biometric encryption, blockchain and visual cryptography. Although it provides cryptographic security, it does not include real-time hazard detection [4]. "The FPGA-Based Light-Weight Encryption for IoMT Devices using ASCON Cipher" [5] discusses light weight encryption to ensure secure data transfer in medical IoT applications. However, it abstains from providing biometric authentication or gas monitoring [5]. The papers "Fast FPGA Reverse Engineering for Hardware Metering and Fingerprinting" [6] and the "FPGA-based Chaotic Cryptosystem" [7] improve FPGA speed and cryptographic security but they do not provide gas detection or biometric authentication. Despite achieving excellent fingerprint recognition accuracy the research paper "Biometric Encryption Using Fingerprint Fuzzy Fault for FPGA-based Embedded Systems" [8] does not assess false acceptance/rejection rates or incorporate real-time environmental monitoring. "Design of Finger Vein Recognition SOC based on FPGA" [9] does not incorporate wireless data transmission or safety compliance, but does not optimize response time and achieve 97% accuracy in finger vein recognition. The studies "Gas Leak Real-Time Detection and Volume Flow Quantification based on Infrared Imaging and Advanced Algorithms" [10] and "Gas Sensing System based on an All-Fiber Photothermal Microcell" [11] does not incorporate security, instead concentrates on gas monitoring in real-time. The research papers "A Study of Drift Effect in a Metal Oxide Sensor and Gas Recognition Using Public Gas Datasets" [12] and "Greenhouse Gas Detection based on Infrared Nanophotonic Devices" [13] discuss infrared-based gas detection and sensor drift but dos not discuss about authentication. The research papers "A Combinational Data Prediction Model for Data Transmission Reduction in Wireless Sensor Networks" [14] improves data and power stability, while "Collective Mapping of Gas Leakages Using Multi-Robot Systems" [15] that supports in leak detection. "Large-Scale Experimental Validation of Real-Time Monitoring in Underground Gas Storage Wells Using Distributed Fiber Optic Sensing" [16] and "Analysis of Gas Leakage Early Warning System based on Kalman Filter and Optimized BP Neural Network" [17] optimizes detection of gas but it does not have biometric authentication. "Gas-Phase Detection of UTI-Causing Bacteria Using Off-the-Shelf Gas Sensors and Change-Point Detection" [18] does not discuss biometric authentication or environmental hazard monitoring, instead it focuses on bacterial detection by gas-phase emissions. "Unmanned Aerial Systems for the Oil and Gas Industry: Overview, Applications, and Challenges" [19] demonstrates the use of drones to monitor gas and gas sector but it does not incorporate biometric authentication. The research paper "Enhanced Electrothermal Analysis for Acetone Gas Detection Based on PolyMUMPs MEMS Sensor" [20] concentrates on MEMS-based on acetone gas detection by using electrothermal actuation but it does not incorporate real-time toluene-detection, biometric authentication, wireless data logging. In contrast, our project combines biometric authentication with real-time gas detection, wireless data transfer and access control. It provides both security and safety by integrating fingerprint-based access control with an automatic system that prevents entry when toluene levels exceed 200 ppm.

Existing research mainly concentrates on cryptographic encryption, biometric authentication and secure IoT data transmission but does not have real-time hazard detection. Cancellable biometric systems use different encryption techniques for protecting fingerprint data but do not monitor environmental safety. Cryptographic authentication methods improve security but do not combine biometric-based physical access control. FPGA-based encryption secures IoT communication but fail to restrict gas-level based access. Biometric security in hardware accelerators prevent hardware piracy but does not have real-time monitoring. This research tackles these gaps by combining biometric authentication with real-time gas detection, facilitating automated access control and assuring safety compliance.

The main objective of this research is to design and implement a Biometric Authentication and Risk Alert System to improve security and safety in chemical laboratories. The system guarantees that only authorized personnel can access restricted areas that constantly monitors toluene levels that prohibit hazardous exposure, activate alerts and prohibits access when unsafe conditions are detected and provides real-time data transmission and logging for continuous monitoring.

This system is mainly designed for chemical laboratories but can be adjusted for other industrial applications. It uses fingerprint-based authentication. These systems may require periodic maintenance for optimal performance. It is necessary to periodically calibrate the gas sensor for accuracy because it measures toluene levels in an efficient but imprecise manner. The system's reliance on Wi-Fi connectivity for data transfer could be problematic in settings where network access is restricted.

II. METHODOLOGY

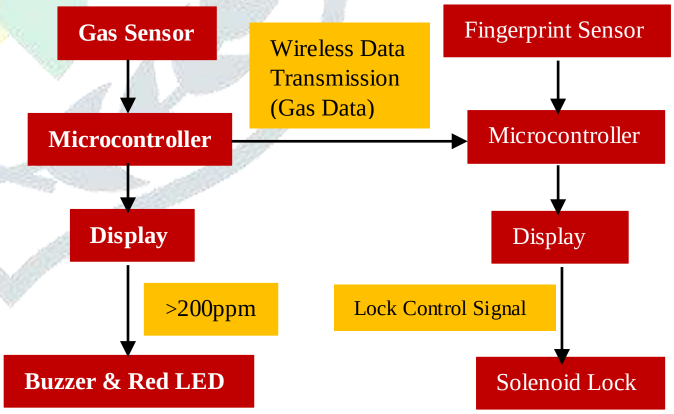


Fig. 1. Block Diagram

A. System Assembly:

- Connect fingerprint sensor, keypad, solenoid lock to the outer system microcontroller, which will be placed outside the laboratory. Outer system is for biometric authentication.
- Connect gas detection sensor to the inner system microcontroller, which will be placed inside the laboratory. The inner system is for gas detection.
- Integrate 2 separate display components to both the systems, one for each system, for displaying fingerprint authentication status and gas concentration levels.
- Connect the buzzer and LED to the gas detection system for alerts.

B. Biometric Authentication:

- Store fingerprints of authorized personnel in the database of fingerprint sensor.
- Upon scanning fingerprint, stored data is being verified by the system.
- If the user is authenticated, the solenoid lock unlocks the door.
- If unauthorized, access is denied and door remains locked.

C. Gas Detection and Risk Alert System:

- The toluene levels in ppm are being continuously measured by gas detection sensor.
- The data from the sensor is sent to microcontroller for processing, and processed data is sent to display component for displaying on it.
- The system triggers buzzer and LED, only if the toluene level exceeds 200 ppm.
- Door remains locked when toluene level exceeds 200 ppm.
- When the level comes below 200 ppm, only then the door is unlocked.

D. Data transmission and monitoring:

- Outer system receives gas concentration data from the inner system wirelessly.
- Whenever user is authorized using fingerprint module, the data like user ID, time is being recorded in the Google Sheets.

E. Testing and Calibration:

- The system is tested under different gas concentration.
- The accuracy of fingerprint authentication is verified with multiple users.

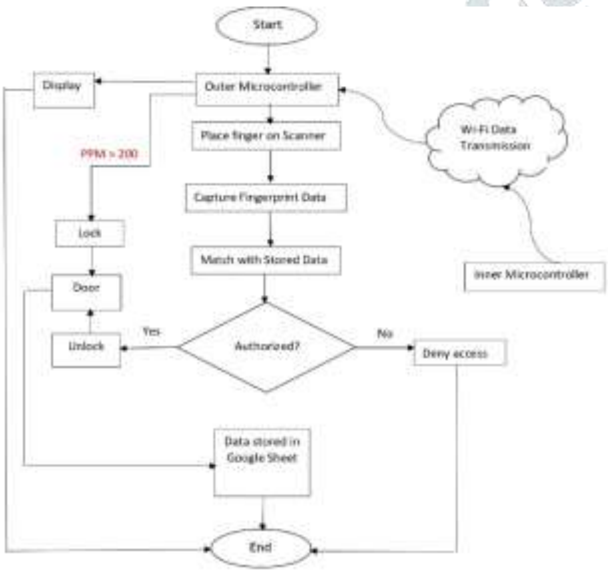


Fig. 2. Outer System Workflow

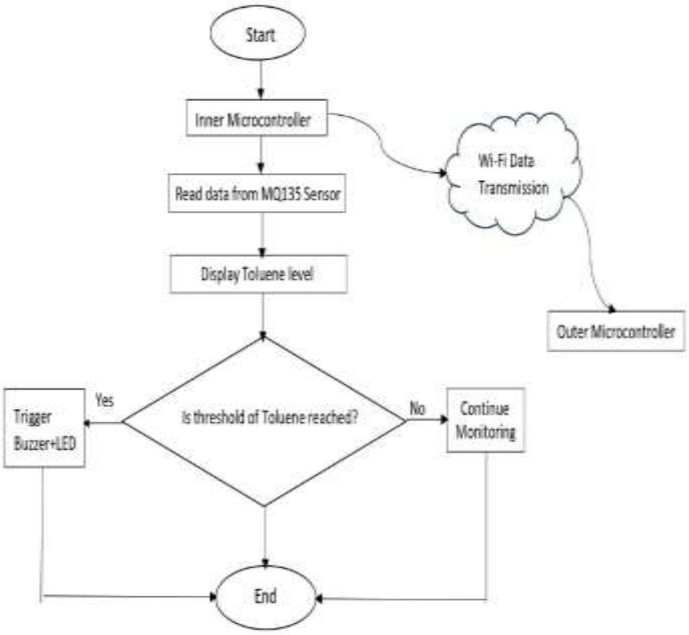


Fig. 3. Inner system Workflow

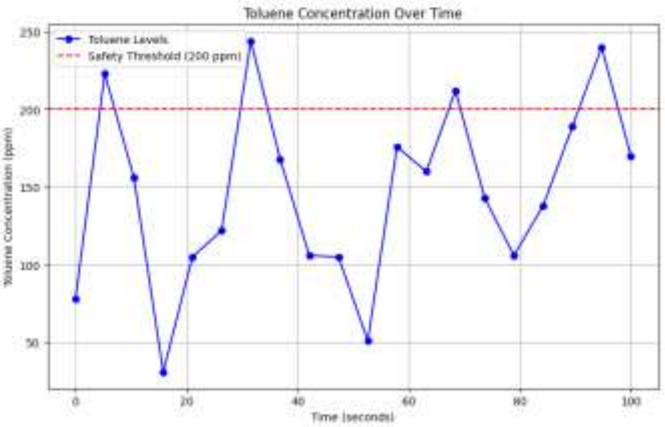


Fig. 4. Toluene Concentration Over Time

The graph depicts the graph depicts toluene concentration (ppm) over time (seconds), with fluctuations representing different exposure levels. A red dashed line at 200 ppm represents the safety level and several peaks beyond this limit indicate potentially hazardous situations.

III. MATHEMATICAL MODEL

A. Biometric Authentication Model:

False Rejection Rate (FRR) and False Acceptance Rate (FAR) can be used to model Biometric Authentication:

$$FAR = \frac{Number\ of\ False\ Accepts}{Total\ Imposter\ Attempts} \times 100$$

B. Access Control Probability Model:

The probability of granting access can be modeled as:

$$P(A) = P(F) \times P(G)$$

Where,

- P(A) = Probability of access being granted
- P(F) = Probability of correct fingerprint match
- P(G) = Probability of toluene level being safe (below 200 ppm).

C. PPM to Scale Conversion:

The concentration of gas in the air is expressed in PPM (parts per million and given as:

$$PPM = \frac{Number\ of\ gas\ molecules}{Total\ number\ of\ air\ molecules} \times 100$$

The resistance (R_s) of gas sensors, such as MQ135, varies with gas concentration, and the relationship between (R_s) and PPM is power-law function.

The resistance (R_s) is provided by the MQ135 sensor in accordance with the gas concentration. Ratio of resistance of the sensor in the presence of gas with respect to clean air resistance R_o is

$$\frac{R_s}{R_o} = A \times PPM^B$$

Where,

- A and B = gas specific constants from the datasheet of the sensor.
- R_o = Resistance of sensor in clean air.
- R_s = Resistance of sensor in presence of gas.
- PPM = Concentration of the target gas.

Therefore, $PPM = \left(\frac{R_s}{R_o}\right)^{1/B}$

We must first convert the analog voltage provided by the sensor to resistance:

$$R_s = R_L \times \left(\frac{V_{CC} - V_{OUT}}{V_{OUT}}\right)$$

Where,

R_L = Load Resistor
V_{cc} = supply voltage
V_{out} = Sensor's analog output voltage

$$R_L \times \frac{\left(\frac{V_{CC} - V_{OUT}}{V_{OUT}}\right)^{1/B}}{R_oA}$$

We normalize PPM using the following in order scale it into a range:

$$S = \frac{PPM - PPM_{min}}{PPM_{max} - PPM_{min}} \times 10$$

Where,
S = ppm value scaled between 0 to 10
PPM_{min} = Lowest Detectable Concentration
PPM_{max} = Maximum Measurable Concentration

$$S = \frac{\frac{R_L \times \left(\frac{V_{CC} - V_{OUT}}{V_{OUT}}\right)^{1/B} - PPM_{min}}{R_oA}}{R_oA} \times 100$$

IV. RESULTS

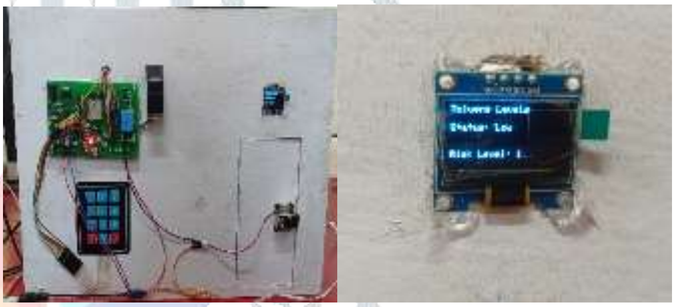
The system was tested in the laboratory. The results showed that biometric authentication was effective, identifying authorized users. The gas detection sensor successfully detected different toluene concentrations and triggered appropriate alerts when necessary. Table 1 summarizes the response of system to different toluene concentrations.

Toluene level (ppm)	Scale	Status	System Response
<10 ppm	0	Safe	Normal Operation
10-50 ppm	1-3	Low	Display Alert
51-110 ppm	4-6	Medium	Warning Message
111-200 ppm	7-9	High	Precautionary Alert
>200 ppm	10	Danger	Buzzer+LED+Door Lock

Table 1. System based on toluene levels

The concentration of Toluene is scaled between 0 and 10. When toluene levels are less than 10 ppm, the lab environment is considered to be safe and the system runs smoothly without any warnings. The system senses low risk and displays warning on the display components that inform lab personals of risks when the toluene levels escalate between 10 ppm and 50 ppm. If the toluene concentration rises between 51 ppm and 110 ppm, the system sends out alert message that indicates moderate risk. At high levels, early warning is initiated, indicating that safety measures should be taken in order to prevent further exposure of people to toluene. When toluene levels exceed 200 ppm, the system triggers critical safety protocols, activating a buzzer, LED, and locks the door in order to minimize exposure to hazardous conditions.

Fig 5. Output Showing Status of Chemistry Lab



In the above Fig. 5, the toluene concentration is below 10ppm, so its scaled value 0 is been displayed on the display component and the status shown is Safe and system continuous with the normal operations.

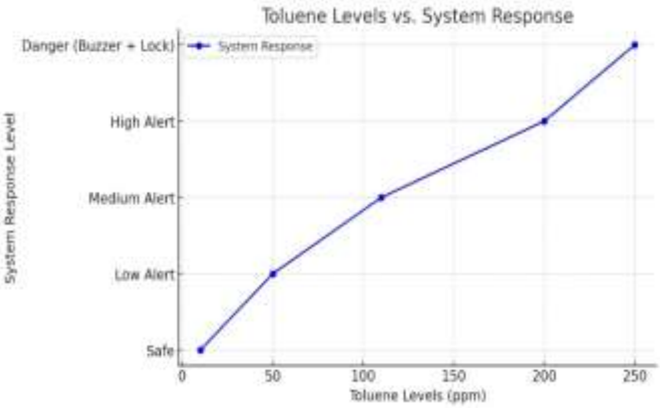


Fig. 6. Toluene levels vs. System Response

Real-time monitoring and wireless data transmission allowed for seamless communication between the gas detection and access control subsystems. The system successfully prevented unauthorized access during hazardous conditions, confirming its suitability for chemical laboratories.

V. CONCLUSION

Chemical lab security and safety measures are successfully integrated by biometric authentication and risk alert system. By employing fingerprint authentication, unauthorized access is prevented, while the gas detection sensor continuously monitors toluene levels. The automated alerting features of the system enhance workplace safety and thus reduces potential health risks. The system is useful for research labs, industries involving chemicals, and educational institutions since it guarantees adherence to safety rules, minimizes response times, and reduces efforts of manual monitoring. To further improve risk assessment and safety measures, future enhancements might incorporate AI-driven predictive analytics and cloud-based monitoring.

VI. REFERENCES

[1] Anirban Sengupta and Mahendra Rathor, "Securing Hardware Accelerators for CE Fingerprinting," *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION SYSTEMS*, vol. 28, pp. 1-8, 2020.

[2] Lamiaa A. Abou elazm, H. Shawkey, Fathi E. Abd El-Samie, Sameh Ibrahim, Mohamed K. H. Elsaid, Mohamed G. Egila and Walid El-Shafai, "Hardware Implementation of Cancellable Biometric Systems," *Proceedings of the Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, pp. 1-8, 2020.

[3] Mohammed Adil Akbar, Mehdi Hamidkhani and Mostafa Sadeghi, "Establishing Security using Cryptography and Biometric Authentication to Counter Cyber-Attacks," *14th International Conference on Information and Knowledge Technology*, pp. 1-6, 2023.

[4] Aakriti Thawre, Ashish Hariyale and B. R. Chandavarkar, "Survey on Security of Biometric Data using Cryptography," *Second International Conference on Secure Cyber Computing and Communication*, pp. 1-6, 2021.

[5] Kamal Raj and Srinivasu Bodapati , "FPGA-based Light-Weight Encryption of Medical Data for IoMT Devices using ASCON Cipher," *IEEE International Symposium on Smart Electronic Systems*, pp. 1-6, 2022.

[6] Anvesh Perumalla , Heiko Stowasser and John M. Emmert, "Fast FPGA Reverse Engineering for Hardware Metering and Fingerprinting," *IEEE National Aerospace and Electronics Conference*, pp. 1-5, 2023.

[7] Anup Kumar Das and Mrinal Kanti Mandal, "FPGA Based Chaotic Cryptosystem," *Second International Conference on Advanced Computational and Communication Paradigms*, pp. 1-6, 2019.

[8] Rabia Bakhteri and Mohamed Khalil Hani , "Biometric Encryption using Fingerprint Fuzzy Vault for FPGA-based Embedded Systems," *IEEE*, pp. 1-5, 2009.

[9] Jie Li, Wenyao Yang, Wenyao Yang and Zedong Nie, " Design of Finger Vein Recognition SOC Based on FPGA," *7th International Conference on Information Science and Control Engineering*, pp. 1-5, 2020.

[10] Man Yan, Zhou Li , Zheng Dong, Yiming Liun, Liyun Chen , Xiaosong Wu and Lijun Wu , "Gas Leak Real-Time Detection and Volume Flow Quantification Based on Infrared Imaging and Advanced Algorithms," *IEEE Open Access Journal*, pp. 1-9, 2025.

[11] Matej Njegovec, Jure Javornik, Simon Pevec, Vedran Budinski, Tomaz Gregorec, Benjamin Lang, Manuel Tanzer, Alexander Bergmann and Denis Đonlagi´, "Gas Sensing System Based on an All-Fiber Photothermal Microcell," *IEEE SENSORS JOURNAL*, pp. 1-11, 2024.

[12] IL-SIK CHANG, SUNG-WOO BYUN, TAE-BEOM LIM and GOO-MAN PARK, "A Study of Drift Effect in a Popular Metal Oxide Sensor and Gas Recognition Using Public Gas Datasets," *IEEE Open Access Journal*, pp. 1-10, 2023.

[13] CHUNHUI HAO, XIAO FU, XIAOYONG JIANG, YUTONG LI, JUYI SUN, HAITAO WU, HE ZHU, QING LI, YUNHAI LI, ZHANGCHENG HUANG, FANG ZHONG, TING HE, JINSHUI MIAO and WEIDA HU, "Greenhouse Gas Detection Based on Infrared Nanophotonic Devices," *IEEE Open Journal of Nanotechnology*, pp. 1-13, 2023.

[14] Khushboo Jain , Arun Agarwal and Ajith Abraham, "A Combinational Data Prediction Model for Data Transmission Reduction in Wireless Sensor Networks," *IEEE Open Access Journal*, pp. 1-13, 2022.

[15] RONNIER FRATES ROHRICH, LUÍS FELIPE MESSIAS, JOSE LIMA and ANDRÉ SCHNEIDER DE OLIVEIRA, " Collective Mapping of Gas Leakages to Determine Safe Routes Using Multi-Robot System," *IEEE Open Access Journal*, pp. 1-21, 2024.

[16] LINQING LUO, DIANA ABDULHAMEED, GANG TAO, TIANCHEN XU, JIANGNAN WANG, DAVID XU, KENICHI SOGA and YUXIN WU, " Large-Scale Experimental Validation of Real-Time Monitoring in Underground Gas Storage Wells Using Distributed Fiber Optic Sensing," *IEEE Open Access Journal*, pp. 1-10, 2025.

[17] GUOQUAN LIU, ZHICHAO JIANG and QI WANG, " Analysis of Gas Leakage Early Warning System Based on Kalman Filter and Optimized BP Neural Network," *IEEE Open Access Journal*, pp. 1-14, 2020.

[18] Christoforos Panteli, Marios Stylianou, Andreas Anastasiou and Chrysafis Andreou, " Gas-Phase Detection of UTI-Causing Bacteria Using Off-the-Shelf Gas Sensors and Change-Point Detection," *IEEE SENSORS JOURNAL*, vol. 24, pp. 1-9, 2024.

[19] THUMEERA R. WANASINGHE, RAYMOND G. GOSINE, OSCAR DE SILVA, GEORGE K. I. MANN, LESLEY ANNE JAMES and PETER WARRIAN, " Unmanned Aerial Systems for the Oil and Gas Industry: Overview, Applications, and Challenges," *IEEE Open Access Journal*, pp. 1-18, 2020.

[20] ABDULLAH S. ALGAMILI, ZMRI ZAINAL ABIDIN, MOHDHARIS BIN MD. KHIR, ABDELAZIZ YOUSIF AHMED, USMAN BATURE ISYAKU and ALI AHMED SALEM, " Enhanced Electrothermal Analysis for Acetone Gas Detection Based on PolyMUMPs MEMS Sensor," *IEEE Open Access Journal*, pp. 1-13, 2024.