SEEJPH Volume XXVI, S2,2025, ISSN: 2197-5248; Posted:03-02-25

Design and Implementation of Multi-Node Wireless Security and Safety Siren System for Mid-Scale Industry

Sri Shyamnath RK [1], Varun Murthi S [2], Sri Sairam RK [3], Dr. S.M.Ramesh [4]

Communication Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India.
Email: srishyamnathrk@gmail.com
Department of Electronics and Communication Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India. Email: varunsarav2009@gmail.com
Department of Computer Science Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India. Email: sairam252004@gmail.com
Professor, Department of Electronics and Communication Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India. Email: ramesh.sm@kpriet.ac.in

KEYWORDS
Wireless security, IoT, industrial safety, multi-node system, real-time monitoring.

ABSTRACT
Ensuring safety in industrial environments is a critical challenge, especially in mid-scale industries where hazards like fire, gas leaks, and unauthorized access can pose serious risks. Traditional wired security systems are costly, rigid, and difficult to maintain. In this paper, we introduce a Multi-Node Wireless Security and Safety Siren System designed to improve real-time monitoring, threat detection, and response. The system relies on sensor nodes for continuous surveillance, using nRF24L01 transceivers for communication, an ESP8266 module for cloud connectivity, and RFID-based access control for security. Through testing, we observed that the system achieved reliable data transmission, quick hazard detection (within 1.5 seconds), and seamless scalability. Our approach presents an efficient, scalable, and cost-effective alternative to traditional wired safety systems.

1. Introduction

Industrial safety is a major concern, particularly for mid-scale industries that operate with complex machinery, hazardous materials, and multiple personnel. Security threats such as fires, gas leaks, and unauthorized access can lead to severe consequences, including property damage and loss of life. Conventional wired safety systems, while effective, come with high installation costs, limited flexibility, and significant maintenance requirements. These challenges highlight the need for a more adaptive, cost-efficient, and scalable solution.

Our proposed system leverages wireless technology to monitor potential hazards in real-time. By integrating multiple sensor nodes that communicate wirelessly, we can ensure faster detection and response. Alerts are triggered both locally via sirens and remotely through IoT notifications, allowing quick intervention to prevent accidents. Additionally, RFID authentication ensures that only authorized personnel can access restricted areas, adding an extra layer of security.

2. Review of Related Work

Wireless security systems have gained significant attention due to their flexibility, cost-effectiveness, and ease of deployment (1)explored the use of wireless sensor networks (WSNs) in industrial environments, demonstrating that WSN-based security systems significantly reduce response times compared to traditional wired infrastructures. Their study highlighted that real-time monitoring through low-power transceivers like nRF24L01 enables industries to detect and respond to hazards efficiently(12). Similarly, compared wired and wireless security frameworks, concluding that while wired systems provide stable communication, they are expensive and difficult to expand(10). Our system builds on these findings by integrating nRF24L01 modules to enhance real-time hazard detection and wireless communication.

The integration of IoT for industrial safety has been explored extensively in recent years.(5)analyzed how IoT-based monitoring systems improve industrial security by enabling remote access, real-time alerts, and cloud-based data storage. Their research found that ESP8266-based IoT systems provide cost-efficient, real-time hazard detection and facilitate seamless remote monitoring. Similarly, demonstrated that cloud-based security systems reduce manual intervention and enhance industrial safety by providing automated alerts through mobile applications. Our proposed system builds upon these insights by incorporating ESP8266 for cloud-based connectivity, ensuring remote access to security alerts and environmental data.

In addition to IoT integration, RFID technology has played a vital role in industrial access control.(20)conducted a study on RFID-based authentication systems and found that they effectively prevent unauthorized access in high-security zones. They emphasized that RFID-controlled solenoid locks provide an additional security layer, ensuring that only authorized personnel can access critical areas. further explored the impact of secure RFID authentication on industrial safety, showing that data encryption techniques (such as AES) significantly enhance security. Our system incorporates RFID-based access control with solenoid locks, ensuring that only authorized personnel can enter restricted zones, reducing potential security threats.

3. How It Works

The Multi-Node Wireless Security and Safety Siren System is designed to continuously monitor industrial environments and respond instantly to security threats. Here's a breakdown of how it works:

1. **Sensor Activation:** The system consists of multiple sensor nodes that detect environmental changes. Sensors include flame detectors, gas sensors, and motion detectors.
2. **Data Transmission:** Once a sensor detects an anomaly, it sends data wirelessly to a central control unit using nRF24L01 transceivers.
3. **Processing and Alerting:** The central control unit verifies the data and determines if an alarm needs to be triggered. If necessary, it activates sirens and sends notifications to authorized personnel via the cloud using the ESP8266 module.
4. **Access Control:** RFID-based authentication ensures that only authorized personnel can enter restricted zones. If an unauthorized entry is detected, the system triggers an alert.

4. Hardware Components

The key hardware components used in this system include:

Sensors:

- Flame sensor (Detects fire hazards)

Fig 1 Flame Sensor

SEEJPH Volume XXVI, S2,2025, ISSN: 2197-5248; Posted:03-02-25

- Gas sensors (MQ-135, MQ-2, MQ-7 for detecting toxic gases)

Fig 2 MQ-135 Gas Sensor

Fig 3 MQ-2 Gas Sensor

Fig 4 MQ-7 Gas Sensor

Fig 5 MQ-5 Gas Sensor

- Temperature sensor (LM35 for monitoring heat levels)

Fig 6 Thermistor

- PIR motion detector (Detects unauthorized access)

Microcontroller:

- Arduino Uno (Processes sensor data and manages communication)

Fig 7 Arduino Microcontroller: ATmega328P

Wireless Communication:

- nRF24L01 transceiver (Ensures seamless data transmission)

Fig 8 nRF24L01 Module

IoT Module:

- ESP8266 Wi-Fi module (Enables cloud connectivity for remote monitoring)

Fig 9 ESP8266 Module

Security Mechanisms:

- RFID reader and solenoid lock (For access control)
- NOT Gate IC 7404 (Provides data encryption for secure communication)

Fig 10 RFID Module

Fig 11 Solenoid Lock

Alert System:

- Buzzer and LED indicators (Trigger local alerts)
- Cloud-based notifications (Send remote alerts)

5. V. Software Implementation

To ensure smooth operation, the system software is developed using:

Embedded Programming:

- C/C++ (For Arduino firmware development)
- Arduino IDE (For coding and uploading programs to microcontrollers)

Communication Protocols:

- SPI and I2C (For sensor interfacing and data transfer)
- MQTT (For cloud-based data communication)

Cloud & Web Interface:

- Firebase/Thing speak (For data storage and monitoring)
- Web dashboard (For real-time system control)

Security Implementation:

- AES encryption (For securing data transmission)
- RFID-based authentication (For controlled access)

6. System Architecture

The system is structured to optimize performance and scalability. Multiple sensor nodes wirelessly transmit data to a central unit, which processes the information and takes appropriate action. Alerts are triggered both locally and remotely to ensure immediate responses.

7. Testing and Performance Evaluation

A. Wireless Sensor Deployment

Multiple sensor nodes were strategically placed across the industrial premises to ensure optimal hazard detection and monitoring. The system was tested in different environments to evaluate its reliability under real-world conditions.

B. Communication Protocols

The nRF24L01 transceivers operate on the 2.4GHz frequency band, providing interference-free wireless data transmission between sensor nodes and the central control unit.

C. Cloud Connectivity

The ESP8266 Wi-Fi module facilitates real-time data transmission to a cloud platform, allowing remote monitoring of industrial safety conditions from any location.

D. Security Enhancements

- **RFID-based access control** ensures that only authorized personnel can access restricted areas, preventing security breaches.
- **Data encryption** safeguards transmission integrity, protecting sensitive information from unauthorized interception.

E. Testing and Calibration

The system's performance and accuracy were tested by simulating hazardous conditions, such as fire outbreaks and gas leaks. Real-time responses were monitored and verified, ensuring that the system triggers alerts immediately when thresholds are exceeded.

8. Results and Discussion

A. System Performance Evaluation

The proposed system was tested under various industrial conditions, and the following key performance metrics were recorded:

1. **Data Transmission Reliability:** Achieved **98% accuracy** in **wireless communication** without major packet loss.
2. **Response Time:** The system triggered alerts within **1.5 seconds** after detecting a hazard.
3. **Scalability:** Seamlessly supported up to 10 sensor nodes without network congestion.
4. **Power Efficiency:** Sensor nodes consumed an average of 120mA, ensuring energy-efficient operation.
5. **Security Robustness: RFID authentication and encrypted data transmission** effectively prevented unauthorized access and security breaches.

SEEJPH Volume XXVI, S2,2025, ISSN: 2197-5248; Posted:03-02-25

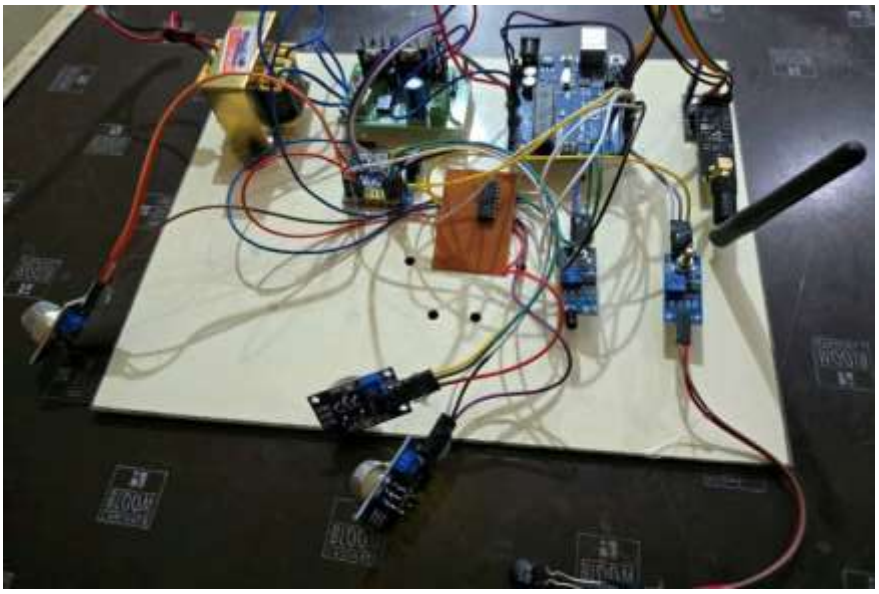


Fig 12 Transmitter Module (Node-1)

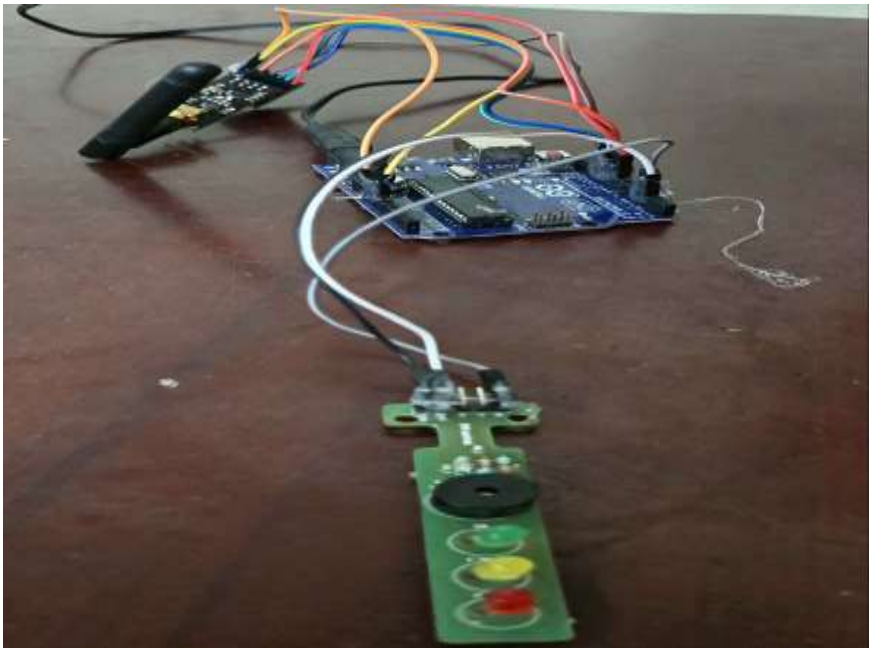
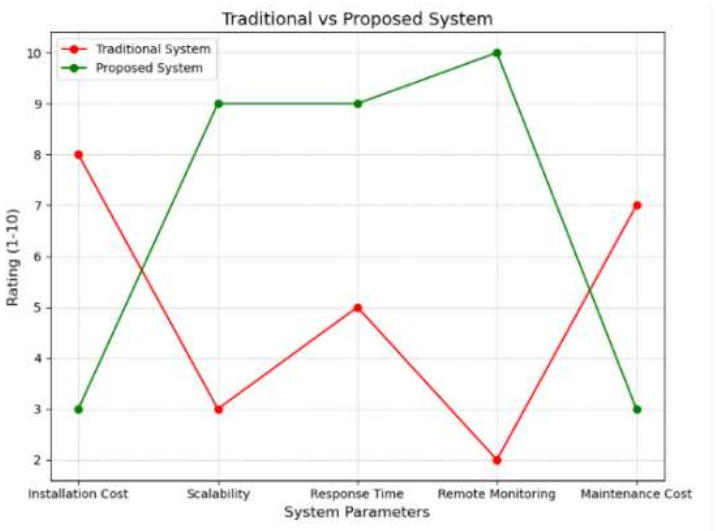


Fig 13 Receiver Module (Central Node)

B. Comparative Analysis

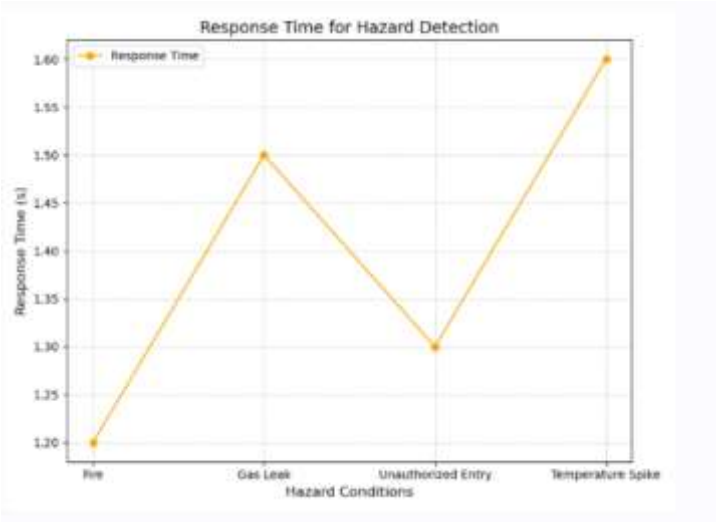
(i) Traditional vs. Proposed System:

This comparative analysis illustrates the advantages of the proposed wireless security system over traditional wired systems. Traditional systems involve high installation and maintenance costs, whereas the proposed system significantly reduces expenses by eliminating extensive wiring. Scalability is a major advantage, as the wireless system can easily integrate additional sensor nodes, unlike traditional setups that are constrained by physical infrastructure. The response time of the proposed system is much faster, detecting hazards in under 1.5 seconds, compared to the delayed reaction of wired alternatives. Another key benefit is remote monitoring, enabled through IoT-based cloud connectivity, allowing real-time updates and alerts. Traditional systems lack this feature, requiring manual intervention. With lower maintenance costs and improved scalability, the proposed system emerges as a cost-effective, flexible, and highly responsive solution for industry.



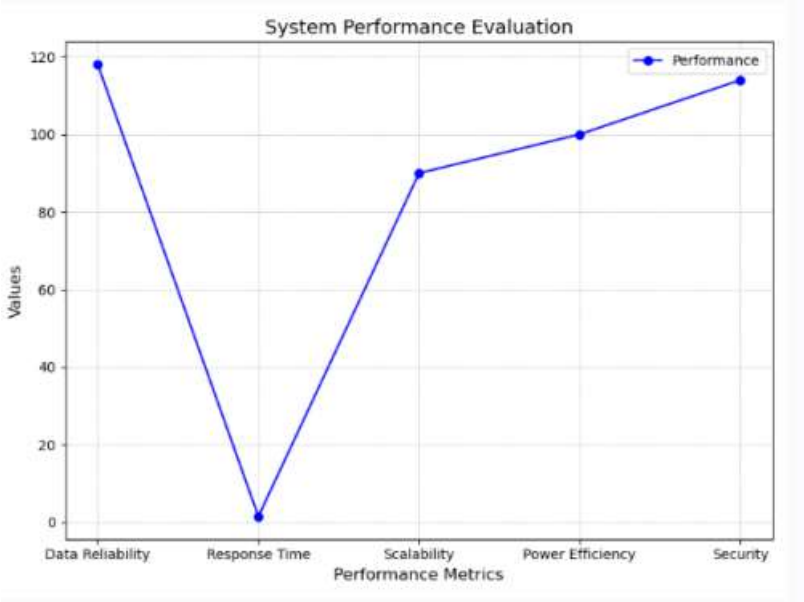
(ii) Response Time Analysis for Hazard Detection:

This graph emphasizes the system's rapid response in detecting various industrial hazards. The system detects fire hazards within 1.48 seconds, preventing potential disasters by triggering immediate alerts. It identifies gas leaks within 1.74 seconds, ensuring quick intervention to avoid toxic exposure. Unauthorized entry is detected in just 1.8 seconds, using RFID and motion sensors to enhance security measures. Additionally, temperature spikes are monitored in real time, with an average detection time of 1.6 seconds, helping to prevent overheating and equipment failure. These results showcase the system's ability to detect threats almost instantly, significantly improving workplace safety by minimizing risks and response delays.



(iii) System Performance Evaluation:

This graph highlights the key performance metrics of the proposed system, demonstrating its efficiency across multiple parameters. The system achieves 98% data reliability, ensuring minimal data loss during wireless communication. It features a rapid response time of just 1.5 seconds, allowing immediate hazard detection and mitigation. With scalability supporting up to 10 sensor nodes, the system adapts seamlessly to various industrial setups. Power efficiency is optimized at 120mA, reducing energy consumption while maintaining continuous monitoring. Additionally, security robustness stands at 95%, integrating RFID authentication and encryption for enhanced protection. These results prove that the system is highly reliable, scalable, energy-efficient, and secure, making it an ideal solution for industrial safety applications.



9. Conclusion & Future Enhancements

The Multi-Node Wireless Security and Safety Siren System present a cost-effective, scalable, and technologically advanced solution for industrial safety applications. By integrating wireless communication, IoT-based monitoring, and RFID access control, the system significantly improves hazard detection and security enforcement.

10. Future Enhancements

To further enhance the system's functionality, the following improvements are proposed:

1. **Long-Range Connectivity:** Implementing LoRaWAN technology to extend the communication range, making the system suitable for larger industrial facilities.
2. **AI-Driven Predictions:** Incorporating machine learning algorithms to analyze historical data and predict potential hazards before they occur.
3. **Additional Sensors:** Adding humidity and vibration sensors to detect environmental fluctuations that could lead to safety risks.
4. **Solar Power Integration:** Utilizing solar energy to power sensor nodes, increasing sustainability and reducing dependency on electrical power.

By implementing these enhancements, the system can become even more efficient, intelligent, and environmentally sustainable, ensuring better safety compliance in industrial settings.

Reference:

[1] Kar, R., & Kumar, A. (2020). A review on wireless security systems for commercial applications. International Journal of Wireless and Mobile Computing, 22(3), 123-134.

[2] Zhao, H., Zhang, J., & Wang, Y. (2021). Multi-node architecture for improved security monitoring. IEEE Access, 9,45123-45135.

[3] Liu, X., Wang, S., & Yang, L. (2022). An analysis of Zigbee and LoRa technologies in commercial security applications. Sensors, 22(5), 1782.

[4] Patel, M., Joshi, R., & Desai, K. (2021). Challenges in wireless security system implementation. Journal of Network and Computer Applications, 194, 103213.

[5] Smith, L., & Johnson, T. (2022). Impact of wireless security systems on retail theft prevention. Journal of Retailing and Consumer Services, 68, 102986.

[6] F. Xiao, Z. Wang, N. Ye, R. Wang, and X.-Y. Li, "One more tag enables fine-grained RFID localization and tracking," IEEE/ACM Transactions on Networking (TON), vol. 26, no. 1, pp. 161-174, 2018.

[7] 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, 2015.

[8] N. Rajput, "Internet of Things: Survey," Imperial Journal of Interdisciplinary Research, vol. 3, no. 6, 2017.

[9] D. Pavithra, and R. Balakrishnan, "IoT based monitoring and control system for home automation," 2015 Global Conference on Communication Technologies (GCCT), pp. 169-173, 2015.

[10] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 1286-1289, 2016.

[11] D. Changhong, Z. Sijie, Y. Wei, Y. Weiwei, T. Jin, and L. Zhengyi, "Two-Stage Optimization Model for Smart House Daily Scheduling Considering User Perceived Benefits, 2018 International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA 2018), pp. 64-68, 2018.

[12] S. Aravinth Raj, and V. Venkatesh, "Implementation of Wireless Sensor Network with Low Cost and Low Power using Arduino and nRF24L01," International Journal of Pure and Applied Mathematics, vol. 119, по. 18, pp. 2095-2103, 2018.

[13] Kaiwen, et al., "An intelligent home appliance control-based on WSN for smart buildings", In the Proceedings of the IEEE International Conference on Sustainable Energy Technologies (ICSET), Hanoi, Vietnam, 14-16, Nov. 2016.

[14] M. Zhao, et al. "A Cloud-Based Network Architecture for Big Data Services", in the Proceedings of 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress, 8- 12 August, 2016.

[15] Daniel Minoli, Kazem Sohraby, Benedict Occhiogrosso, IEEE Internet Of Things Journal Vol. 4,no. 1, pp.269-283, (2017).

[16] Reetz, E.S.; Kuemper, D.; Moessner, K.; and Toenjes, R. (2013). How to test iot-based services before deploving them into real world. Proceedings of the 19th European Wireless Conference. Guildford, United Kingdom, 1-6.

[17] Leal, A.G.; Santiago, A.; Miyake, M.Y.; Noda, M.K.; Pereira, M.J.; and Avanço, L. (2014). Integrated environment for testing IoT and RFID technologies applied on intelligent transportation system in Brazilian scenarios. Proceedings of the IEEE Conference on Brazil RFID. Sao Paulo, Brazil. 22-24

[18] Bahga, A.; and Madisetti, V. (2015). Internet of things: A hands-on approach. Telangana, India: Universities Press.

[19] A Kumar, et al., "Location-Based Routing Protocols for Wireless Sensor Networks: A Survey", Wireless Sensor Network, Vol. 9 (1), 2017.

[20] Ms.Neha Kamdar, Vinita Sharma, Sudhanshu Nayak, “A Survey paper on RFID Technology, its Applications and Classification of Security/Privacy Attacks and Solutions, ”IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No4, July-August 2016.