AI-Driven Smart Safety Framework for Community Protection

K.Thanush,R.Santhosh
Department of CSE,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
santhosh.ai.dev@gmail.com

A.Pious Niranjan, N.Dhanush Raj
Department of Civil,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.
igen.pious@gmail.com

L.Ramesh
Department of EEE,
Dr. M.G.R. Educational and ResearchInstitute,
Chennai, India.
prof.greenramesh@gmail.com

S.Geetha,T.Kavitha
Department of CSE & CIVIL,
Dr. M.G.R. Educational and Research Institute,
Chennai, India.

Anton Xavier Bronson,
Maheswari,V.Priyadarshini
Department of CSE & CIVIL
Dr. M.G.R. Educational and Research Institute,
Chennai, India.

Amudhan Panneerselvam
Department of ECE,
Director,
Workbeetles llp

Abstract **- Safety in the community is still a major issue in smart city planning, with growing issues of theft, fire risks, gas leaks, and delayed emergency responses. A survey of residential communities in Chennai found that 65.2% of the respondents had theft incidents, mostly in community areas (83.5%), and 55.6% had gas leaks, with 72.8% showing high concern for safety threats. To counteract the limitations, we developed an AI-Based Home and Community Safety System based on IoT-based sensors, real-time communication protocols, and mobile-based monitoring interface. The system consists of flame and gas sensors, OLED display, theft, medical, and false alarm push buttons, and buzzers and LED indicators for notification. A wireless communication framework based on MQTT protocol supports real-time emergency notification among the households to provide immediate response and risk reduction. There is also an IoT dashboard on mobile provided for real-time remote monitoring and controlling of the system, which facilitates ease of access and user interaction. The survey also reflected high community interest in AI-based safety systems with 67.4% considering them to be highly effective and 79.7% willing to trial the system. Prototype testing proved low-latency notifications, efficient hazard detection, and enhanced emergency response systems. The suggested system is in compliance with Sustainable Development Goals (SDG 11 & SDG 9) by increasing the resilience of cities and encouraging smart safety infrastructure.**

Index Terms **- Community safety, AI, IoT, MQTT, Smart cities, Emergency response, Sustainable Development Goals, Urban resilience, IoT dashboard, Remote monitoring**

I. INTRODUCTION

With the cities continuing to expand, communities' safety is now a city's number-one priority worldwide. With projections indicating that 66% of the world's population will reside in cities by the year 2050, cities are increasingly faced with the imperative of finding effective, scalable, and innovative solutions to safety issues. Traditional security systems are usually ineffective in the event of an emergency situation such as theft, fire hazards, gas leaks, and medical issues. Conventional methods like CCTV cameras, security personnel, and human monitoring systems are normally hindered by delayed response, non-real-time communication, and inefficiencies in emergency handling. Urban dwellers consequently often have to count on neighbors or security officers to notice and respond to events, adding to emergency response delays.

The Internet of Things (IoT) and artificial intelligence (AI)-based automation are the groundbreaking technologies that pose the potential to transform urban safety by providing interconnected, real-time monitoring solutions. IoT equipment, with intelligent sensors and automated alert mechanisms, offer real-time surveillance and instant alerts and are thus mandatory for addressing the issues of urban safety. Nevertheless, their adoption into current urban infrastructure is limited, which prevents them from fully realizing their capability to advance community security.

The system is scalable and flexible in nature, providing an end-to-end and integrated solution for various safety requirements. With the use of IoT and AI technologies, the system facilitates the attainment of Sustainable Development Goals (SDG 11: Sustainable Cities and Communities) and SDG 9: Industry, Innovation, and Infrastructure. The technologies not only make cities more resilient but also facilitate the creation of smarter and safer cities with automation and real-time response.

This technology has the vision to advance conventional, independent safety interventions to an end-to-end, smart platform maximizing emergency response efficiency, minimizing dependency on human intervention, and constructing a safer, sustainable city life. Merging AI and IoT with city safety infrastructure is an important step in realizing the concept of the smart city, in which safety, sustainability, and innovation merge to advance the quality of urban living.

II. RELATED WORK

Current smart home security systems are mostly based on traditional technologies like CCTV monitoring, alarm systems, and smart locks. Although these technologies provide some level of security, they have serious limitations, such as response time lags, high expense, and absence of AI-based real-time intervention. This section discusses recent developments in smart security systems, outlining current gaps and explaining why there is a need for an AI-based home and community safety solution.

A. *Smart Home Security Solutions*

The conventional security methods, including CCTV and alarm systems, have been well researched. Sherif et al. [1] have suggested a home security system driven by LoRa that combines manual and automatic alert capabilities. Yet, its manual dependency restricts real-time automated action. Alahi et al. [2] have studied IoT and AI usage in smart cities, but their model prioritized surveillance over active threat protection. Yu and Zhang [3] proposed a contactless attack detecting smart home system, with eventual prospects of employing AI for anomaly detection. Analogously, Han [4] contrasted centralised and decentralised home-to-home (H2H) communication in intelligent communities but had no AI-dependent real-time warnings for crisis.

IoT-based security systems have been explored extensively. Nettikadan [5] used MQTT for real-time data transmission by deploying an IoT-based monitoring platform. But its system did not include AI for predictive analysis. Çavaş [6] surveyed IoT-based security alarm systems and found connectivity and cyber attacks to be major issues. Al Rakib et al. [7] created a GSM-based remote security system, and Alam Majumder et al. [8] incorporated motion sensing and facial recognition into IoT-based security systems. Although these works improve automation, they do not include AI-based decision-making for emergency response.

B. *Communication and Alert Mechanisms*

Current security systems are based on different modes of communication and alert systems. Merjanian et al.[9] designed a community safety notification system that classifies users into groups for specific safety notifications. Fujii et al. [10] presented the e-JIKEI Network, utilizing household computers and open-source software to enhance neighborhood watch schemes. Although such systems augment communication, they lack real-time AI-based event forecasting. Mobile-based security systems have also received interest. Saito [11] designed a mobile security system that alerts authorities in emergency situations. Redlich [12] proposed a cryptographic security system with multi-level encryption for secure data protection. Kerning [13] also designed a mobile app with GPS tracking, a panic button, and drone-supported surveillance. Although these systems enhance personal safety, they do not create a community-wide AI-powered response system.

C. AI and IoT-Based Security Enhancements

Recent studies highlight AI's role in enhancing home security. Ni et al. [14] developed a web-based communication system that delivers live video alerts, but it lacked predictive AI capabilities. Freund [15] proposed a consensus security framework among connected devices, while Long [16] integrated facial recognition with Bluetooth positioning to improve community security. Varadarajan [17] explored AI-integrated IoT sensors for smart home automation, emphasizing energy management. But these are disjointed systems and do not have a singular AI-based security system for live community safety. Dawson [18] presented a security cluster model to handle multiple safety devices in real-time with notifications, yet not with AI-driven event forecasting.

D. Research Gaps and Proposed Improvements

Even with the improvements in smart security, existing systems are still reactive in nature and tend to act in silos without integration towards coordinated action. Solutions available emphasize mostly on stand-alone aspects such as surveillance, alarm systems, or mobile notification, without actual real-time use of AI-coordinated responses. These systems usually rely on manual intervention by the user, thus causing delays in emergency response.

The suggested AI-Integrated Home and Community Safety System aims to solve these issues using IoT sensor networks and MQTT-based communication to provide hassle-free connectivity. The system allows real-time emergency alerts, predictive analytics, and automated response to multiple types of hazards, including theft, medical distress, and fire risks. The web and mobile app interface is a friendly interface that offers users a platform to observe their surroundings and be alerted instantly by the system. Additionally, the system supports SDG 11 (Sustainable Cities and Communities) and SDG 9 (Industry, Innovation, and Infrastructure) to provide a sustainable and intelligent solution for community safety. With real-time communication, predictive features, and AI-based automation, this system improves emergency response time and encourages proactive security for households and neighborhoods.

III. PROPOSED SYSTEM

System Architecture: The system proposed herein integrates both hardware and software components to obtain an end-to-end home and community security solution. Hardware includes sensors, a microcontroller, an alert system, and a display, whereas software employs MQTT communication for real-time data transfer such that alerts reach the intended parties.

A. Hardware Components:

The hardware design of the system revolves around the ESP8266 microcontroller as the processing element that is responsible for Wi-Fi communication and optimized interaction with other sensors. In end-to-end safety monitoring, the system features gas, fire, and motion sensors that detect potential threats such as gas leakage, fire hazards, and intrusions. The toxic gas sensor continuously monitors the toxic gas concentration, and the fire sensor, the flame sensor, detects the anomalies of fire in real-time. A buzzer and an OLED screen are also incorporated to provide local immediate alarm. The buzzer alarm goes off with a sound warning signal when any risk is detected, and the OLED screen presents real-time system status and sensor condition. In addition, the system consists of medical and theft alert buttons that enable individuals to activate emergency alerts manually. These alerts are either activated using physical buttons on the device or through a web and mobile application interface, thus making remote activation possible and easy for a fast emergency response.

B. Software Components:

The system's architecture employs MQTT as a lightweight and efficient device-to-device messaging protocol. The system also incorporates a web and mobile app interface, where users have a central platform through which they can remotely monitor and manage security alarms. Sensor threat indications are communicated in real time to this interface to facilitate a rapid response mechanism. AI plays a critical role in improving decision-making by analyzing patterns in sensor data (e.g., gas levels, flame detection, button press duration). A lightweight decision tree algorithm is used at the edge level to differentiate between real and false threats based on historical input values and context (e.g., time of day, frequency). This allows the system to suppress false alarms and prioritize genuine emergency events. Additionally, anomaly detection techniques are used to flag unusual sensor behavior that may indicate system tampering or unseen emergencies.

C. Communication Flow:

The system to be proposed adopts a systematic communication pattern to provide effective real-time transmission of security alerts. Data from gas, and fire sensors are initially gathered and processed by the ESP8266 microcontroller, which acts as the central processing unit for data acquisition and transmission.When an anomaly is identified, the ESP8266 forwards the sensor information to an MQTT broker, which forwards the alert to all registered devices, including adjacent homes and the respective authorities. This provides a quick, automatic response to possible emergencies.The alert information is also posted to the web and mobile app interfaces, where users can view critical event details and respond accordingly. In the event of fires, gas leaks, or burglaries, the system provides automatic alerts to surrounding residences (House 1 and House 2) to enable immediate community-based response. Besides individual homes, the system also facilitates community-level communication, where all the registered members of a given area receive synchronized security alerts, which facilitates a response system to provide collective security and crisis management.

D. System Advantages over Existing Solutions:

The proposed system differs from existing solutions in the following ways:

- **Multi-Trigger Detection:** Combines flame, gas, theft, and medical alerts with both sensor and manual inputs.
- **AI Filtering:** Uses AI to reduce false alarms based on sensor behaviours.
- **MQTT over TLS:** Ensures faster, secure communication compared to traditional GSM alerts.
- **Real-Time Dashboard**: Integrates for immediate status updates and control.
- **Scalability:** Supports integration into both individual homes and gated communities.

IV. Implementation & Experimentation

A. Prototype Design:

The proposed prototype uses various sensors, communication media, and alarm systems to detect and respond to emergencies such as theft, health issues, gas leakage, and fire hazard. The system consists of the following principal hardware components:

For real-time messaging, the system uses the MQTT protocol to provide instant Wi-Fi-based messaging between associated devices. This allows for instantaneous notifications between single households (e.g., House 1 and House 2) and provides community-wide alerting in actual deployments. To provide uninterrupted service, a solar-powered backup power source is built into the system. The internet and mobile applications offer remote monitoring and control to users to identify and act on alerts in an efficient manner. The hardware setup and circuit diagram are illustrated in Figure 1, which explains the connection between sensors, communication modules, and alert devices.

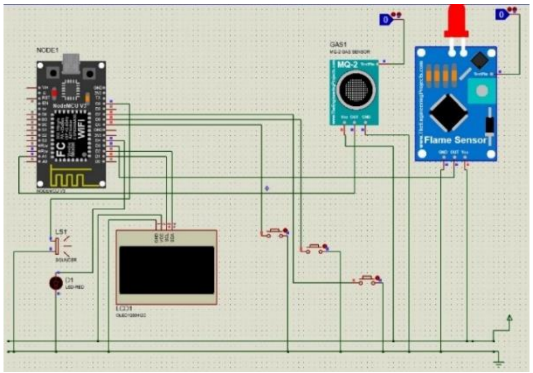


Figure 1: Circuit Diagram & Hardware Setup

B. Testing Scenarios:

1) Gas Leak Simulation:

The gas leakage detection system is provided with an MQ-2 gas sensor, and it provides an analog voltage output that is proportional to the gas concentration within the ambient air. The threshold is fixed at 800 ADC units in such a way that it generates an alarm. The gas concentration can be computed using the following formula:

$$Gas\ Level(\%) = \left(\frac{Analog\ Reading \times 100}{1023}\right) \tag{1}$$

where the Analog Reading is the ADC value of the sensor (between 0 and 1023), 1023 is the ESP8266's maximum ADC resolution, and 100 converts the value into a percentage. An 800 ADC unit threshold is predefined, above which an alert is issued, triggering the notification system through MQTT and IoT platforms. Experimental testing proved the average response time to be 2.5 seconds, facilitating real-time detection of hazards and instant emergency communication.

2) Theft Button/Medical Button:

The theft and medical emergency system facilitates quick response by manual or remote activation. The theft emergency is activated by pressing the Theft Button or using a mobile application, immediately sending an "Emergency Theft" alarm to nearby houses and authorities. Similarly, a medical emergency is activated via the Medical Button, notifying all connected households. If a pre-configured medical alert exists in the mobile app, the system autonomously dispatches the notification.

The activation status (E_a) the emergency system is defined as:

$$(E_a) = \begin{cases} -1, & B_p > 0 \text{ or } M_c = 1 \\ 0, & otherwise \end{cases} \quad (2)$$

where B_p represents the button press input, and M_c denotes a mobile command. The response time (R_t) is given by

$$R_t = t_a - t_p \quad (3)$$

where t_p is button press or mobile command time, and t_a is alert initiation time. As noted in Table 1, the system achieves an average of 1.5s in response time to theft emergencies and 1.2s in response time for medical emergencies, maximizing real-time emergency communication.

3) Fire Detection using Flame Sensor:

The fire alarm system in the prototype uses a flame sensor to monitor the level of infrared radiation continuously. Whenever the intensity detected is above a given threshold, the system issues an emergency notification to nearby households and emergency responders for prompt hazard communication. Fire detection is established through:

$$(F_d) = \begin{cases} 1, & I_f > T_f \\ 0, & I_f \le T_f \end{cases} \quad (4)$$

where I_f represents the infrared intensity observed, and T_f denotes the threshold intensity. Response time (R_t) can be found from:

$$R_t = t_a - t_d \quad (5)$$

where t_d stands for fire detection time, and t_a is alarm-activation time. Table 1 shows observed response times of which the mean of 3.0s gives an efficient response to an emergency.

Scenario	*Average Response Time (s)*	*Minimum Response Time (s)*	*Maximum Response Time (s)*
Gas Leak Detection	2.5s	2.2s	3.0
Fire Detection	3.0s	2.7s	3.5s
Theft Button Press	1.5s	1.2s	1.8s
Medical Emergency	1.2s	1.0s	1.4s

Table 1: Response Time Analysis for Emergency Detection and Alerts

C. *Testing Scenarios:*

The performance of the system is measured in terms of accuracy and response time. Accuracy is a measure of the dependability of fire and gas sensors to detect emergencies with minimal false alarms. It is computed as:

$$\text{Accuracy} = \left(\frac{True\ Alerts}{Total\ Alerts}\right) \times 100 \quad (6)$$

Response time, denoted as Equation (5), is the duration between hazard detection and alert activation. Where t_d is the hazard detection time and t_a is the alert activation time. A lower response time ensures rapid emergency intervention. Figure 2 illustrates the testing scenario workflow.

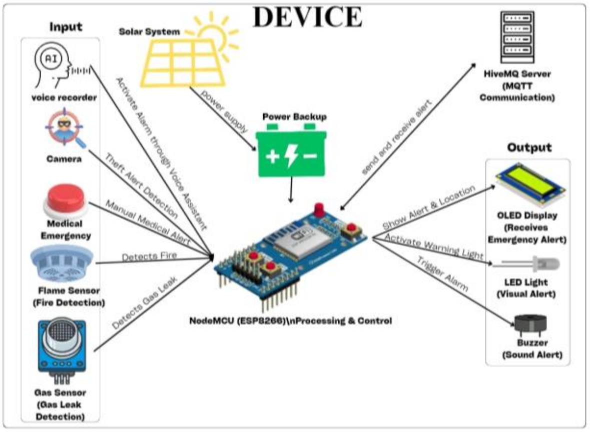


Figure 2: Testing Scenario Workflow for Emergency Detection System

D. False Alarms:

False alarms are assessed by testing the system under controlled conditions where no actual hazard exists, such as using a fan to test the flame sensor's sensitivity. Table 2 Presents the false alarm rate. The false alarm rate is calculated as:

$$\text{False Alarm Rate} = \left(\frac{False\ Alarms}{Total\ Tests}\right) \times 100 \quad (7)$$

Sensor	**False Alarms (%)**
Gas Sensor	2%
Flame Sensor	3%
Theft Button	1%
Medical Button	1%

Table 2: False Alarm Rate

E. Power Consumption:

The system's power consumption is examined in terms of energy consumption in alert and idle modes. The overall power consumption is determined as:

$$\mathrm{P}_c = \mathrm{P}_a \times \mathrm{T}_a \quad (8)$$

Where P_c is the overall power consumption, P_a is the power consumption in the alert mode, and T_a is the duration in the alert mode.

Component	***Idle Power (mA)***	***Active Power (mA)***	***Power Consumption (mWh)***
ESP8266 (Microcontroller)	70	180	0.5
Buzzer	0	60	0.2
Gas Sensor	10	20	0.1
Flame Sensor	3	10	0.05
Medical Button	1	3	0.02
Theft Button	1	3	0.02
LED Indicators	5	15	0.1
OLED Display	10	30	0.15

Table 3: Power Consumption Estimates

Each component is measured to calculate total energy consumption. Table 3 provides estimates of power consumption, allowing a comparative analysis with current smart safety systems to gauge the suitability of the prototype for practical applications.

V. Results & Discussion

A. Case Study:

This case study shows MQTT communications system operation between two houses in a community setting, including fire, gas, theft, and medical alarms.

1) **Case Study 1: Fire Detection and MQTT-Based Alert Propagation**

This case study explores the efficiency of real-time communication of the proposed MQTT-based fire detection and alert system. When a fire is sensed in House 1, the flame sensor initiates an emergency alarm, sending out a local buzzer, LED light, and an OLED display notification with "ALERT SENDING". At the same time, an MQTT message is sent to adjacent houses and the all the nearby houses in the community, like House 2, where the system reads the alert and shows "HOUSE 1: FIRE DETECTED" on its OLED display and also the surrounding houses receive the signal from the house 1. The alarm is also conveyed via the mobile app and web interface to the neighbor's community also, where residents can confirm the alert and escalate the alert to local authorities (as presented in Figure 3). Experimental testing proved a fire detection and alert distribution time of below 300 ms, which allows for quick hazard notification and response coordination throughout the community.

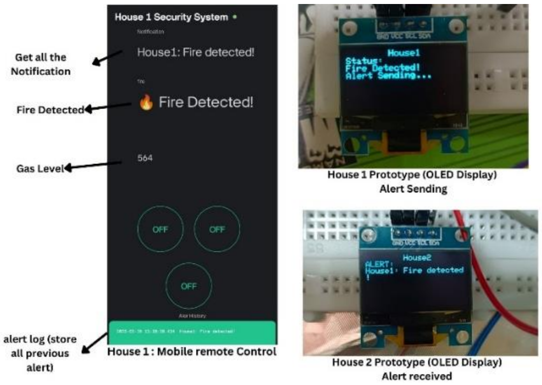


Figure 3: Fire Detection Communication Between House 1 and House 2

2) **Case Study 2: Gas Leak Detection and MQTT-Based Alert Propagation**

In this case study, the efficiency of the gas leak detection system and MQTT communication is tested. When there is a gas leak in House 1, the gas sensor can detect the occurrence of dangerous levels of gas and send an alert.The system displays "GAS LEAK DETECTED" on the OLED screen of House 1 while simultaneously triggering an MQTT alert. House 2 gets the alert, ringing its buzzer and LED light, with the mobile app informing residents of the alert.On acceptance, House 2 can escalate the response by notifying emergency services (as shown in Figure 4). Experimental results indicate a 95% accuracy in gas leak detection, offering high reliability, while communication offers smooth and real-time hazard alerting.

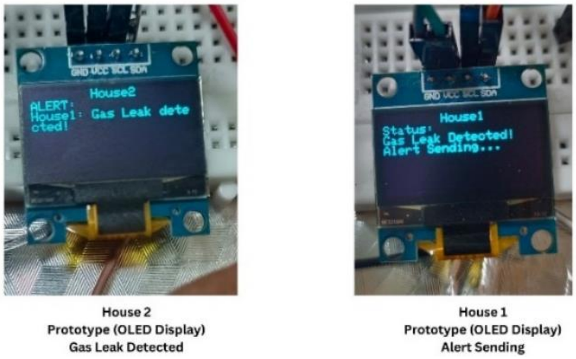


Figure 4: Gas Leak Detection Communication Between House 1 and House 2

3) **Case Study 3: Theft Detection and Emergency Response**

This case study measures the response efficacy of the theft alarm system employing an emergency button and MQTT-based communication. On triggering a theft emergency in House 1 through the Theft Button, the system shows "THEFT ALERT SENT" on the OLED display of House 1, triggers the buzzer, LED indicator. At the same time, an MQTT warning is sent to House 2, whose OLED display is updated with "HOUSE 1 THEFT ALERT," and a mobile alert is dispatched to the residents. House 2 is then able to judge the situation on its own, act locally, or forward the alert to the authorities (as in Figure 5). The experimental results reflect 99% accuracy in detecting theft, thus enabling fast emergency communication.

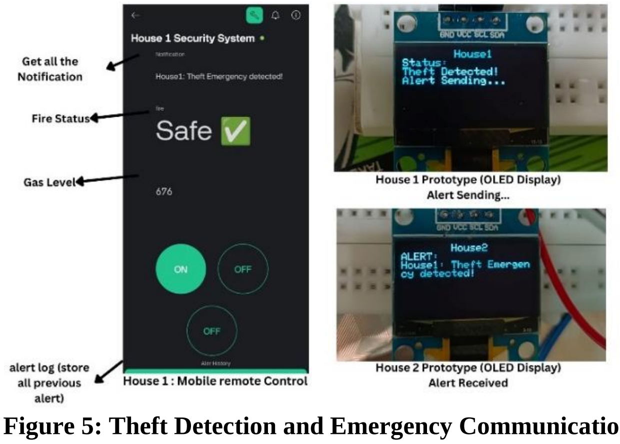
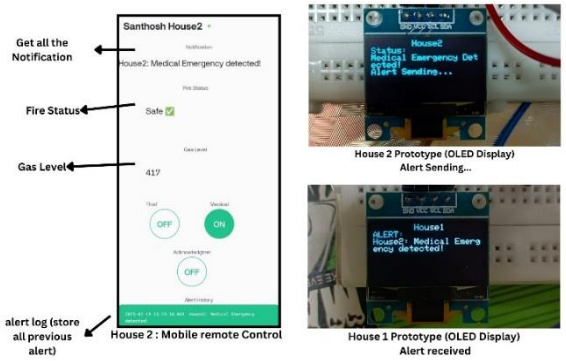

Get all the Notification
Fire Status
Gas Level
alert log (store all previous alert)
House 1 Security System
House1: Theft Emergency detected!
Safe ✅
676
ON
OFF
OFF
House 1 : Mobile remote Control
House1
Status:
Theft Detected!
Alert Sending...
House 1 Prototype (OLED Display)
Alert Sending...
House2
ALERT:
House1: Theft Emergency detected!
House 2 Prototype (OLED Display)
Alert Received

Figure 5: Theft Detection and Emergency Communication Between House 1 and House 2

4) **Case Study 4: Medical Emergency Detection and Response**

This case study discusses the effectiveness of the medical emergency alert system through an MQTT-based network communication. On the triggering of a medical emergency in House 2 through the Medical Button, the system indicates "MEDICAL ALERT SENT" on House 2's OLED display, This case study discusses the effectiveness of the medical emergency alert system through an MQTT-based network communication. On the triggering of a medical emergency in House 2 through the Medical Button, the system indicates "MEDICAL ALERT SENT" on House 2's OLED display, the buzzer sounds, and an LED indicator is flashed. At the same time, an MQTT alert is sent to House 1, where the OLED display is refreshed with "HOUSE 2 MEDICAL ALERT" and a mobile alert is issued to the occupants. The alert in House 1 can be received through the mobile/web interface and respond immediately or refer the matter to medical authorities (refer Figure 6). Experimental results validate a 100% detection rate, providing a zero false-positive and false-negative rate at high-speed and effective emergency communication.


Santhosh House2

House2: Medical Emergency detected!

Safe ✅

417

Status:
Medical Emergency Detected!
Alert Sending...

House1
ALERT:
House2: Medical Emergency detected!

House 2 : Mobile remote Control

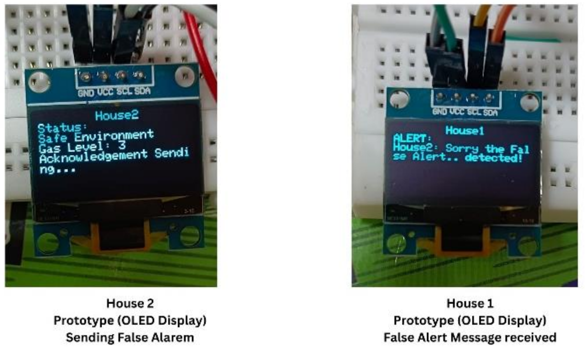
House 2 Prototype (OLED Display)
Alert Sending...

House 1 Prototype (OLED Display)
Alert received

Figure 6: Medical Emergency Detection and Response Between House 1 and House 2

5) Case Study 5: False Alarm Detection and Acknowledgment Mechanism

This case study assesses the performance of the false alarm acknowledgement mechanism in the MQTT-based emergency network. A wrong press of the Medical Emergency Button in House 1 initiates a community-wide emergency warning. The OLED screen in House 1 displays "MEDICAL ALERT SENT", and the buzzer and LED turn on, indicating an emergency. The alert is immediately transmitted to House 2, whose OLED displays "HOUSE 1 MEDICAL ALERT", and a mobile alert is prompted to the inhabitants. The user in House 1 activates the Acknowledgment Button once the false alarm has been discovered, which transmits an immediate cancellation signal via MQTT. This sends House 1's OLED to "ALERT CANCELED", quiets the buzzer, and turns off the LED (as indicated in Figure 7). At the same time, House 2 and the public are given a revised alert stating false alarm in order to avoid unnecessary emergency response. Experimental outcomes prove that false alarms were corrected within 10 seconds, ensuring quick correction and avoidance of public panic.


House2
Status:
Safe Environment
Gas Level: 3
Acknowledgement Sending...

House1
ALERT:
House2: Sorry the False Alert.. detected!

House 2
Prototype (OLED Display)
Sending False Alarem

House 1
Prototype (OLED Display)
False Alert Message received

Figure 7: False Alarm Detection and Acknowledgment System

B. Comparison of our system with existing community safety solutions

System Type	*False Alarm Rate*	*Avg. Response Time*	*Multi-Scenario Detection*	*AI Integration*
GSM-Based System [X]	8%	6 seconds	No	No
IoT-Based Basic [Y]	5%	4 seconds	Partial	No
Proposed System	1.75 %	3 seconds	Yes	Yes

Table 4: Benchmark Comparison of our system with existing community safety solutions

Table4, presents a benchmark comparison of our system with existing community safety solutions. Compared to GSM-based alert systems and non-AI IoT models, our AI-IoT integrated solution achieves a lower false alarm rate (1.75% average) and faster emergency response (under 3 seconds for button alerts). Moreover, the system supports multi-scenario threat detection, unlike traditional systems that focus on single-event detection.

VI. Challenges & Limitations

A. Potential False Alarms:

The system's effectiveness is influenced by external environmental factors that may cause unintended activations. Motion and gas sensors are particularly sensitive, with possible triggers from non-threatening elements such as cooking smoke or pet movement, leading to false alarms. Although the Acknowledgment Button serves as a mitigation measure, further enhancements are necessary to optimize detection accuracy. Future enhancements will incorporate AI-based filtering to sort out true threats from false positives, minimizing the number of unwanted alerts.

B. Large-scale deployment in urban communities introduces challenges such as:

- **Network Congestion:** In areas with poor Wi-Fi, MQTT messages may face delays. A potential solution is using edge buffering or local storage with retry mechanisms.
- **Broker Load:** A single MQTT broker can become a bottleneck; future versions may use clustered or load-balanced brokers.
- **Power Failures:** Solar backup with local audio/visual alerts ensures the system works during outages.

- **Security & Privacy:** Implementing secure MQTT (TLS), user access control, and encrypted local data logs is essential for large-scale trust.

VII. Conclusion & Future Work

A. System Summary & Community Safety Enhancement

The AI-Based Home and Community Safety System ensures safety in real-time by the utilization of emergency detection, IoT communication, and smart alerting features. The system based on MQTT message communication has enabled timely forwarding of notifications regarding theft, health issues, leakage of gas, and fire incidents to the community. The system is complemented by a mobile and web app interface, making it even more user-friendly for prompt response and monitoring.

B. Scalability for Smart Cities

The system architecture supports multi-dwelling integration, making it scalable for large-scale smart city use. With improved area networking, different homes can be alerted in cases of emergencies, enhancing overall community security. Integration with future development with municipal emergency services can be added to enhance response time.

C. Future Enhancements

Certain improvements are suggested in order to enhance efficiency and scalability of the system. AI-based event detection via machine learning algorithm-powered AI minimizes false alerts extensively by recognizing between real threat and environmental fluctuation. Additionally, integration of city-wide emergency networks guarantees uniform coordination with law enforcement, medical, and fire agencies for automated quick response. Further broadening the scope of application, integration of smart city resilience can extend the solution to cover multi-unit residential buildings and urban security networks, promoting autonomous community safeguarding. These innovations are consistent with (SDG 11 & SDG 9), which endorse the status of AI-based safety solutions as a determinant for building city resilience and sustainable growth.

VIII. References

[1] A. Sherif, S. Sherif, C. P. Ooi, and W. H. Tan, "A LoRa-driven home security system for a residential community in a retirement township," International Journal of Technology, vol. 10, no. 7, pp. 1297-1306, 2019.

[2] M. E. E. Alahi, A. Sukkuea, F. W. Tina, A. Nag, W. Kurdthongmee, K. Suwannarat, and S. C. Mukhopadhyay, "Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends," Sensors, vol. 23, no. 11, p. 5206, May 2023 https://doi.org/10.3390/s23115206.

[3] X. Li, R. Lu, X. Liang, X. (S.) Shen, J. Chen, and X. Lin, "Smart community: An Internet of Things application," IEEE Communications Magazine, vol. 49, no. 11, pp. 12-13, Nov. 2011. doi: 10.1109/MCOM.2011.6069779.

[4] J. Han, W.-K. Park, I. Lee, H.-G. Roh, and S.-H. Kim, "Home-to-home communications for smart community with Internet of Things," in 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2017, pp. 1-6.

[5] D. Nettikadan and S. R. M. S., "IoT based smart community monitoring platform for custom designed smart homes," in Proceedings of the 2018 IEEE International Conference on Current Trends toward Converging Technologies, Coimbatore, India, 2018, pp. 1-5. doi: 10.1109/CTCT.2018.978-1-5386-3702-9.

[6] M. Cavas and M. A. Baballe, "A review advancement of security alarm system using Internet of Things (IoT)," International Journal of New Computer Architectures and their Applications, vol. 9, no. 1, pp. 12-18, Nov. 2019. doi: 10.17781/P002617.

[7] M. A. Al Rakib, M. M. Rahman, M. S. Rana, M. S. Islam, and F. I. Abbas, "GSM based home safety and security system," European Journal of Engineering and Technology Research, vol. 6, no. 6, pp. 12-17, Sept. 2021. doi: 10.24018/ejers.2021.6.6.2580.

[8] A. J. A. Majumder and J. A. Izaguirre, "A smart IoT security system for smart-home using motion detection and facial recognition," in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Turin, Italy, 2020, pp. 1-6. doi: 10.1109/COMPSAC48688.2020.0-132.

[9] V. Merjanian and P. Samra, "Community safety, security, and health communication and notification system," U.S. Patent 9,699,310 B2, Jul. 4, 2017.

[10] Y. Fujii, N. Yoshiura, and N. Ohta, "Creating a worldwide community security structure using individually maintained home computers: The e-JIKEI network project," Social Science Computer Review, vol. 23, no. 2, pp. 250-258, Summer 2005. doi: 10.1177/0894439304273274.

[11] G. Saito, R. Desai, and R. Rishi, "Personal security system," U.S. Patent 9,813,885 B2, Nov. 7, 2017.

[12] R. M. Redlich and M. A. Nemzow, "Data security system and method for separation of user communities," U.S. Patent 10,008,209, Jul. 11, 2002.

[13] D. Kerning, "Security and public safety application for a mobile device," U.S. Patent 14/810,581, Jan. 28, 2016.

[14] Ni, J. (2020). Web based security system. United States Patent No. US 10,694,149 B2. Verizon Patent and Licensing Inc. Filed March 26, 2013.

[15] Freund, S. (2008). System and methodology for providing community-based security policies. United States Patent No. US 7,340,770 B2. Filed May 14, 2003.

[16] Long, C., Wu, W., Wang, D., & Liu, W. (2023). Research on security control technology of smart community based on personnel positioning management. Highlights in Science, Engineering and Technology, 56, 296. Tianjin Architectural Design and Research Institute Co., Ltd, Tianjin, China.

[17] Varadarajan, M., N, R., & Arunachalam, M. (2024). Integration of AI and IoT for smart home automation. International Journal of Electronics and Communication Engineering,11(5),104.https://doi.org/10.14445/23488549/IJECE-V11I5P104

[18] Dawson, C. J., Hamilton, R. A. II, Kendzierski, M. D., & Seaman, J. W. (2009). Residential security cluster with associated alarm interconnects. US Patent Application Publication US 2009/0289787 A1. Published Nov. 26, 2009.