KAMPALA INTERNATIONAL UNIVERSITY

KIU
Journal of Science, Engineering and Technology

KJSET Research Article

# Development of a real-time panic alert system using threshold-based audio detection

**Dimple T. Ariyo[1]*, Isaac Ojomuyide[2], Ibrahim K. Ogundoyin[3], Kudirat O. Jimoh[4], John O. Adeniran[5]**

[12345] *Department of Computer Science, Faculty of Computing and Information Technology, Osun State University, Osogbo, Nigeria.*
*dimple.ogunbiyi@uniosun.edu.ng, ojomuyide2000@gmail.com, ibraheem.ogundoyin@uniosun.edu.ng, kudirat.jimoh@uniosun.edu.ng, john.adeniran@uniosun.edu.ng*

*Corresponding Author: dimple.ogunbiyi@uniosun.edu.ng*

**Paper history:**
Received 27 July 2025
Accepted in revised form 13 December 2025

**Keywords**
*Panic Alert System; Threshold-Based Audio Detection; Arduino; IoT; Network Latency; Emergency Response.*

## Abstract

*This study presents the development and evaluation of an IoT-based real-time panic alert system for emergency situations using a threshold-based audio detection method and mobile network communication. The system integrates a voice sensor, Arduino micro-controller, GSM module, cloud-based real-time database, and an Android mobile application to enable automatic panic detection without requiring manual user activation. Short audio frames are continuously captured, and their amplitude values are compared against a predefined panic threshold derived from literature-reported panic-level vocal intensities and experimental testing. System performance was evaluated under the conditions: quiet room, office noise, and street noise, using both human voice input and a calibrated 100 dB sound source. Performance testing was conducted over 2G, 3G, and 4G mobile networks across 100 trials per network type. The results show mean alert latencies of 3.8s, 2.1s, and 1.2s for 2G, 3G, and 4G networks, respectively, with corresponding reliability values of 85%, 92%, and 97% for alerts delivered within 10s. The system recorded a false positive rate of 7% and a false negative rate of 9% during testing. The results demonstrate that combining a simple threshold-based audio detection approach with IoT connectivity and GSM messaging can provide timely and reliable panic alerts, particularly in scenarios where users may be unable to manually trigger emergency notifications.*

**Nomenclature and units**

| | |
|---|---|
| $ADC$ | Analog to Digital Converter |
| $UART$ | Universal Asynchronous Receiver/Transmitter |
| $dB$ | Decibel (Sound Intensity) |
| $Hz$ | Hertz (Frequency) |
| $L_i$ | Latency |
| $L^{-}$ | Mean Latency |
| $R$ | Reliability |

## 1.0 Introduction

Panic is a feeling of fear that usually triggers severe physical reactions. Emergency scenarios such as shootings, stampedes, and fires cause panic. Panic is a common problem and happens often (Alsalat et al., 2018). Emergency situations can be uncovered through panic (Lazarou et al., 2022), and a vital indicator of panic is speech/sound like distress sounds, screams, voice tone/pitch, etc. (Sagar et al., 2022). Advancements in technology have allowed the development of real-time emergency detection and monitoring systems utilizing a variety of intelligent concepts such as IoTs, sensors, etc. (Fitriyan and Syafii, 2024; Damaševičius et al., 2023; Whitmore et al., 2015).

Traditional security measures, such as panic detection button alarms, have been widely used to communicate panic situations and are usually static, meaning they do not actively sense environmental conditions, requiring active user interventions (Ogunbiyi et al., 2023a). Studies have shown the application of IoT sensors, portable electronic devices and intelligent techniques in detecting and communicating situations such as panic/emergency situations. Additionally, early work in voice activity detection employed energy and amplitude checks within short frames. For example, Venkatesh et al. (2021) developed a security warning system for women. The Arduino-powered system has the ability to send SMS alerts to the victims' loved ones when an attack is being detected. Similarly, Chandra et al. (2023) developed a safety alert system using a GSM/GPRS modem, Arduino, a voice module and a buzzer. The system uses two methods for activation: voice commands and pressing a button, which triggers a loud buzzer and sends location information to friends.

Also, Jayanthi et al. (2022) developed an Arduino-based Women Safety and Security System (ABWSSS) with GPS & GSM modules that will transmit emergency information to those who can help. In addition, Ananthula et al. (2022) proposed a GPS-based safety system with dual security features over voice and SMS transmission on a mobile device. A button is designated for use when in danger. The moment the button is pressed, the entire system is engaged, and an SMS with the recipient's location using GPS and GSM is sent right away. Kalbande et al. (2023) discussed a system that can be started by hitting an emergency button once. When the button is pressed, an RF transmitter transmits position information to the police station in the form of latitude and longitude. Using GPS, the victim's position can be found. The GSM modem is used to send SMS. In order to determine the victim's location, an Arduino UNO is interfaced with an RF transceiver on the receiving side. Some other instances include vehicle monitoring, such as in Awodeyi et al. (2018), where a security emergency panic button alarm system for real-time monitoring of security emergencies was developed. It was designed to offer in-depth monitoring of various security emergency situations. The device installed in the car was created using Arduino and ultrasonic sensors to identify any unauthorized access. Also in healthcare, research has been carried out on individual health monitoring and emergency detection, such as reported in (Ruman et al., 2020; Nduka et al., 2019; Mohanty and Mishro, 2023). Existing panic detection systems primarily rely on user-activated triggers such as buttons or apps. These approaches can be ineffective in high-stress conditions where users may be unable to initiate help requests. Prior work (e.g., Venkatesh et al., 2021; Chandra et al., 2023) has explored voice-activated alerts but often lacks real-time integration with cloud systems or mobile apps.

Several reviewed studies use push buttons; however, many users cannot reach a button during panic events. Audio-based triggers can support such cases. Additionally, there are limited studies that test audio amplitude triggers on small devices for panic alert uses and measure end-to-end latency from audio detection to cloud receipt. This study addresses these limitations by integrating a passive, voice-based detection system with GSM communication and Android applications for real-time response. This study developed an audio-based trigger that sends alerts through both a cloud link and a GSM link. The study presents specifically the (i) design of an Arduino-based panic detection system, (ii) implementation of the software and hardware components of the system, and (iii) testing the performance of the system.

## 2.0 Materials and Methods

his section presents the design and implementation process for the software and hardware modules of the system, including the panic detection mechanism. The implementation procedure adheres to the designed framework as defined in the block diagram in Figure 1 in order to achieve the aim of this study. As illustrated, the real-time panic detection system uses a microphone, an ESP8266 module, and a SIM800L module. The microphone feeds raw audio to the ESP8266. The ESP8266 samples audio at a rate of 8000 Hz. The code groups samples into frames of 256 samples and computes the mean absolute amplitude for each frame. The system checks if the value crosses a set limit. When the limit is crossed, the ESP8266 sends a short alert message to a cloud service. The SIM800L sends an SMS to a defined phone number. The embedded micro-controller program runs, initializing the entire system and connecting the system to the cloud server.

The GSM module was also configured to send messages to recipient mobile numbers configured in the embedded program code. The mobile app designed for this system has two parts: the user mobile app and the personnel mobile app. The Android mobile device receives or sends data to a real-time database using a Firebase private key address and a mobile application-linked Uniform Resource Locator (URL).

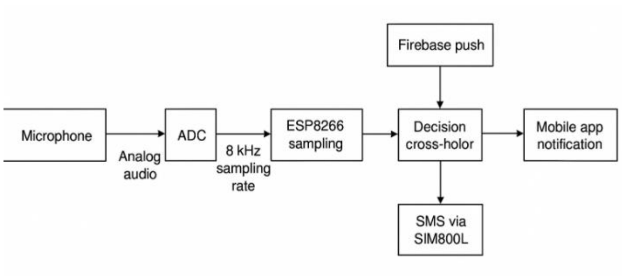



**Figure 1:** Block Diagram of the Real Time Panic Alert System.

## 2.1 Hardware Module

The hardware uses an ESP8266 board, a SIM800L module, and a simple microphone sensor. The board connects the microphone output to the ADC pin of the ESP8266. The SIM800L connects to the ESP8266 through UART. The hardware runs on a 5V supply with a regulator for stable input. The ESP8266's positive terminal was connected to the positive of the power source, and the GND pin was also linked to the GND of the power supply. As shown in Figure 2, the ESP8266 TX and RX were interfaced with the TX and RX of the GSM module, its Vcc pins were linked to the output power supply (+4.2V), and its GND pins were connected to the corresponding 0V supply. The source code was created using the Arduino IDE and then compiled. The hex file was loaded into the Flash memory of the micro-controller. The microcontroller runs a hex file that the compiler generates. The executable code was created by grouping the sequence of zeros and ones into words that were 12, 14, or 16 bits wide, depending on the micro-controller's design. Every word is interpreted by the CPU as an instruction that it is carrying out while it is in operation.

## 2.2 Software Module

The development of software for this system was divided into two forms, viz., embedded program and mobile app software. Arduino C programming was used to program IoT. The code was compiled into a hex file and loaded into the micro-controller's Flash memory. The micro-controller executes the hex file generated by the compiler. The executable code consists of a sequence of zeros, ones and hexadecimal numbers and the MIT inventor was used to create the mobile app that would receive data or send data to the cloud.

The creation of the user interface for a mobile application is also part of the software implementation process. An interactive graphical user interface serves as the user interface for mobile applications. The software interface accepts the voice of a person and sends the information to the micro-controller to determine the status of the panic situation.

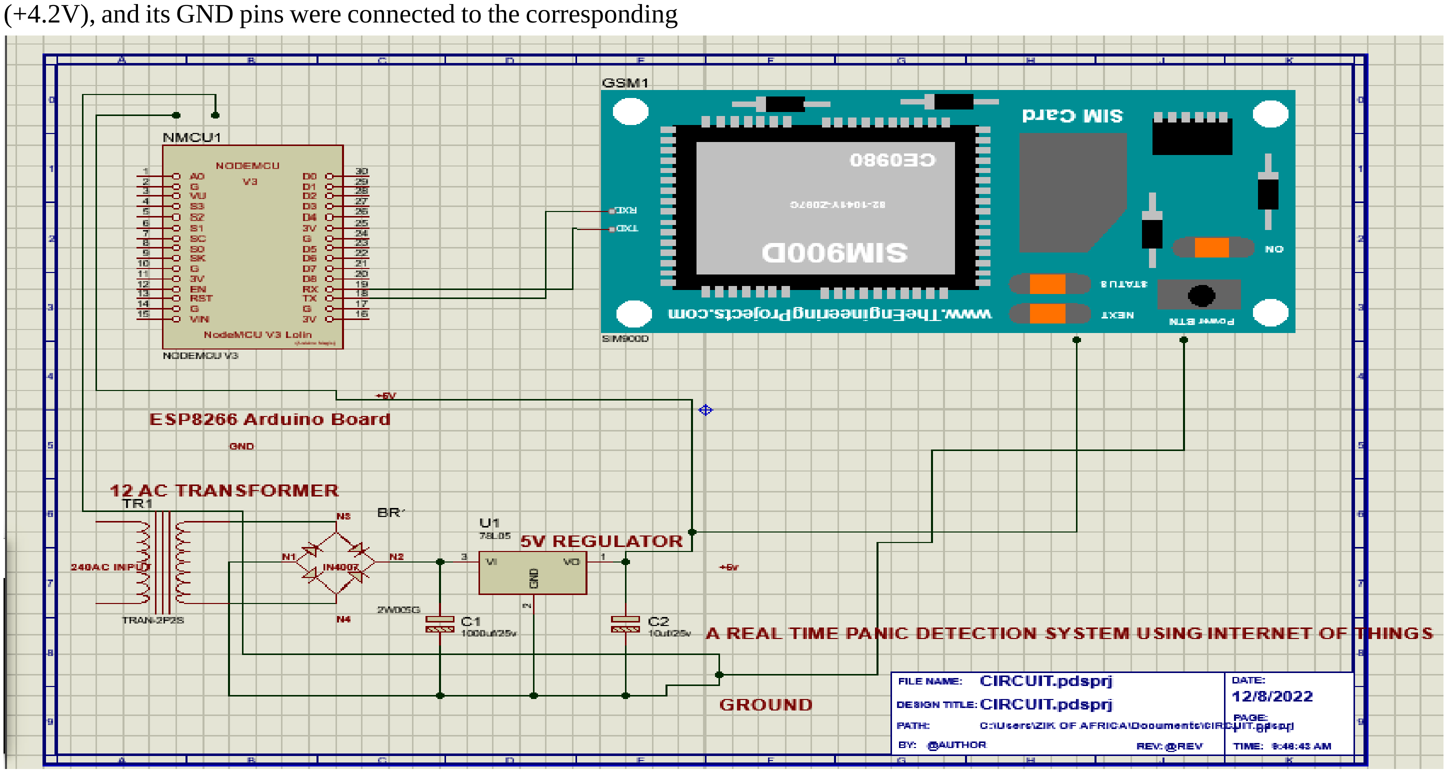



**Figure 2** Circuit Diagram for the System.

## 2.3 Panic Alert Algorithm

A threshold-based voice amplitude method was used to detect a panic situation. Amplitude values are collected from the voice sensor (microphone) and indicate panic when a sequence of amplitude values read exceeds the threshold value, which in this study is set at 100 decibels (dB). The flowchart for the panic alert system is given in Figure 3. The voice sensor outputs an analogue signal whose magnitude depicts the intensity of ambient sound. This analogue signal is periodically sampled by the ESP8266 micro-controller. To reduce false alarms from other loud sounds, the algorithm aggregates multiple readings within a time frame. The algorithm operates in detection cycles where it samples a fixed number of amplitude values. If a set threshold number of those samples exceeds the amplitude level, the system signals a panic event. This method is used to ensure that alerts are issued only when there is sufficient intensity in the voice, such as screaming or crying for help, is detected. The threshold value of 100 dB was determined from literature as a standard range between 100 to 120 dB of sound intensity (Uwuigbe, 2017; John et al., 2017; Ogunbiyi et al., 2023b).

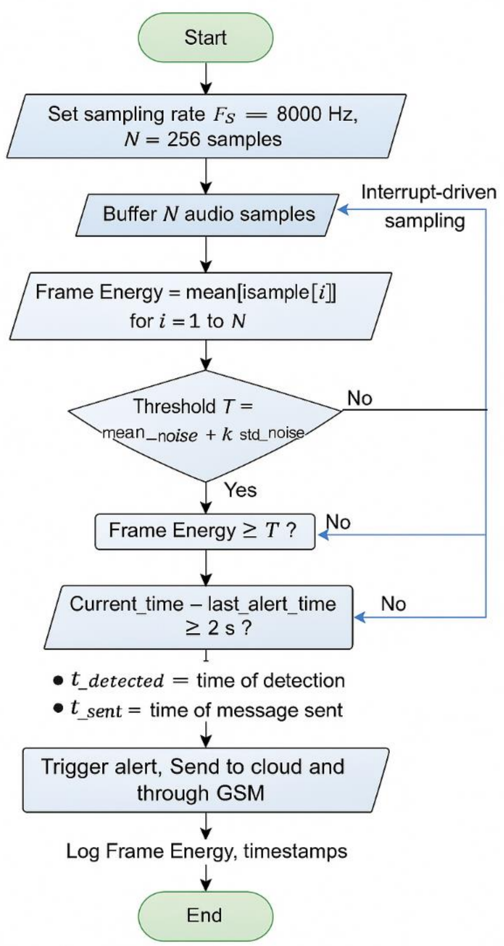



**Figure 3** Real Time Audio Detection Algorithm.

## 2.4 Evaluation

The study used three network types: 2G, 3G, and 4G. Each network had 100 trials. Tests were run in a quiet room, an office with background noise, and a street-level noise setting. The device was placed 1m from the sound source. A human subject and calibrated speaker produced a 100dB signal.

The system recorded T_detected (time the phone app detected panic) and T_received (the time the phone app received the alert). Latency was calculated as $L_i = T_{received} - T_{detected}$ in seconds. Reliability showed the share of alerts received within 10s. The study also measured false positive and false negative rates. Mean, standard deviation, and the 95% CI for the mean was computed using $\bar{L} \pm 1.96(\sigma/\sqrt{N})$. A t-test checked differences across networks. The latency and mean latency were calculated using Equations (1) and (2):

$$Latency\ (L_i) = T_{received}(s) - T_{detected}(s) \quad (1)$$

$$Mean\_latency\ (\bar{L}) = \frac{1}{N}\sum_{i=1}^{N} L_i \quad (2)$$

Reliability was calculated using Equation (3):

$$Reliability\ (R) = \frac{1}{N}\sum_{i=1}^{N} I\,(L_i \leq 10s) \times 100 \quad (3)$$

Where *I( )* is the indicator function.

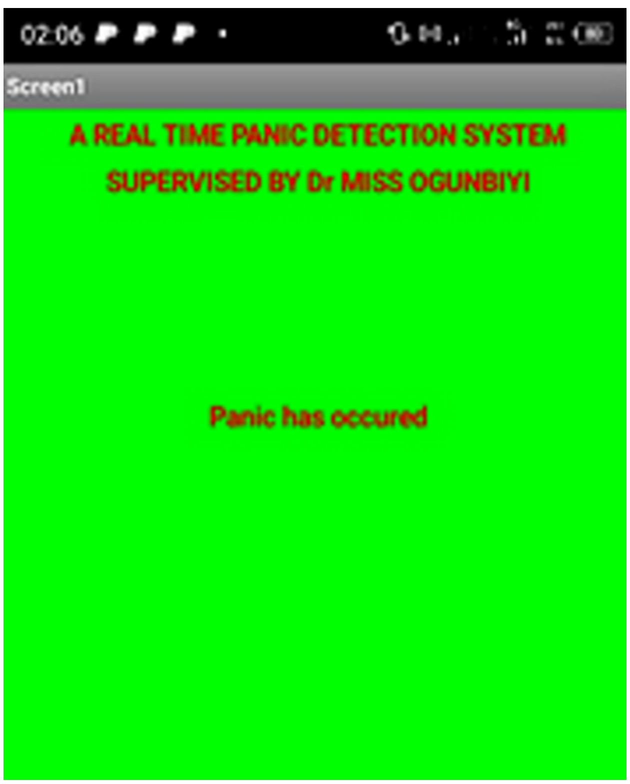
## 2.5 Ethics

The study used consent forms for all human subjects. The system stored only time logs linked to each event. The study removed personal details from all data files. Raw audio was discarded after the extraction of amplitude features.

# 3.0 Results and Discussions

The system joins a simple threshold audio method with real-time cloud and GSM alerts and reports full latency, reliability, and error rates under controlled trials. The hardware modules were assembled on a custom PCB. Firmware was uploaded via Arduino IDE, and the Android app was installed on a smartphone running Android 11. The result obtained using a real-time database for testing the system was displayed on a mobile phone. The voice source interface on the application was used to capture audio voice transmitted to the cloud, as shown in Figure 4. Each module was tested for expected results and also to determine whether each of the modules can interact to transfer data from the micro-controller to the cloud and to the mobile phone in the form of SMS. Figure 5 shows the coupled system with the GSM module and the sample output SMS when panic has been detected. Table 1 shows the alert delivery performance for 2G, 3G, and 4G, including mean latency, standard deviation, and the share of alerts received within 10 seconds. Table 2 shows the sound detection performance of the system, including the share of correct detection, false positives, and false negatives across all tests.

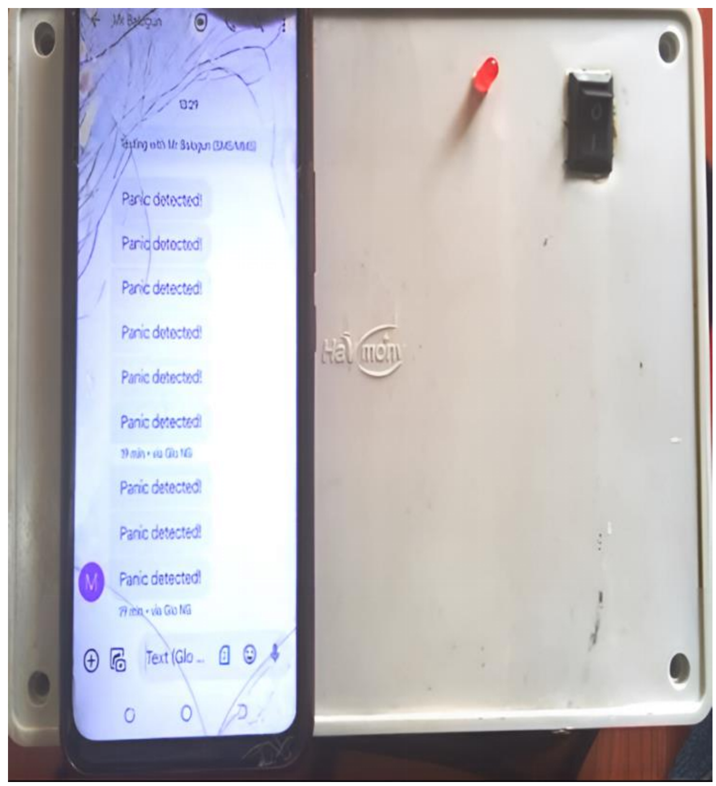

(a)




(b)

**Figure 4** Software Prototype (a) Voice Source Interface and (b) Detection Interface.

(a)




(b)

**Figure 5** Coupled System (a) GSM Module and (b) SMS Output Interface.

**Table 1** Latency and Reliability Results for 2G, 3G, and 4G (N = 100 each).

| Network | Mean (s) | SD (s) | 95% CI (s) | Median (s) | Reliability (%) |
|---|---|---|---|---|---|
| 2G | 3.8 | 0.88 | [3.64, 3.94] | 3.72 | 85 |
| 3G | 2.1 | 0.62 | [2.02, 2.22] | 2.06 | 92 |
| 4G | 1.2 | 0.28 | [1.16, 1.22] | 1.18 | 97 |

**Table 2** False Positive and False Negative Results (N = 100 each)

| Event type | Count tested | Count incorrect | Rate (%) |
|---|---|---|---|
| False positive | 100 | 14 | 7 |
| False negative | 100 | 18 | 9 |

The results analyzed were obtained as recorded in Table 1. The table shows the network status analyses of each network: 2G, 3G and 4G. The system was most responsive under 4G conditions, with an average latency of 1.2 seconds and 97% reliability and minimal delay in cloud update and SMS delivery. Figures 6 and 7 show the charts for the Mean latency and reliability results, respectively. These results show that the system is most effective in environments with faster network infrastructure, pointing out the influence and significance of communication bandwidth on real-time emergency systems. Also, the system performance varied with noise levels, with more missed events during street noise tests, indicating a need for better filtering or adaptive threshold tuning.

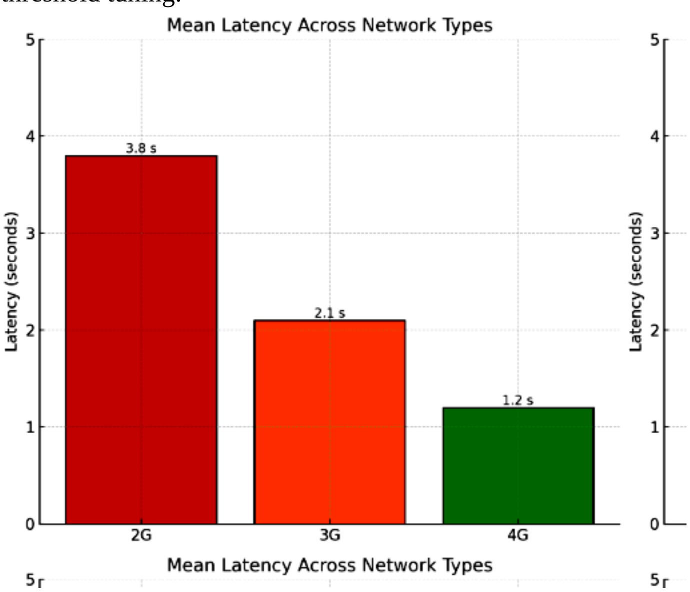



**Figure 6** Mean Latency Across Network Types.

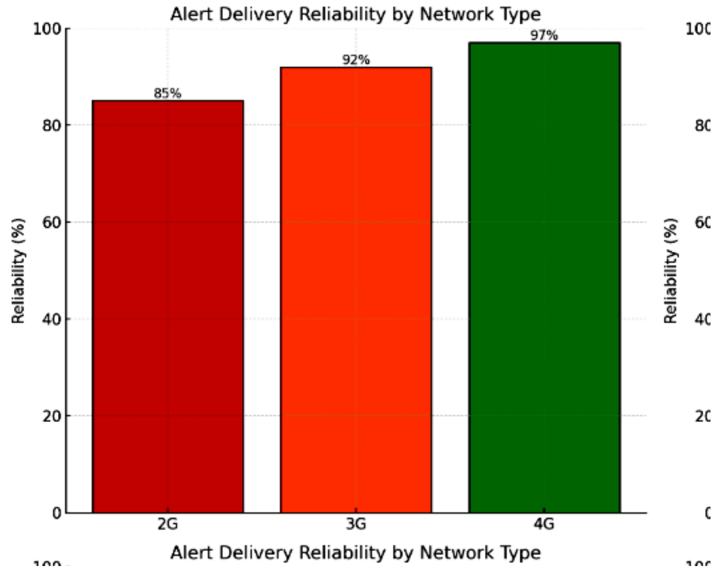



**Figure 7** Alert Delivery Reliability by Network Type.

## 4.0 Conclusions

A real-time panic detection system was designed and implemented, offering a dependable, cost-effective, and user-friendly solution to enhance safety in emergency scenarios. It monitors the environment for panic signals through a human voice and sends real-time alerts. The technology has the potential to make a substantial impact on society. Threshold-based audio detection and GSM modules play a vital role in the design to foster communication between the system, cloud and mobile phone for successful data transfer for both input and output results. The system uses a fixed or adaptive limit that can miss low-volume events and can trigger alerts in complex noise conditions, and also where internet connectivity is poor. The network comparison shows that mobile network quality strongly affects alert delivery time. Future improvements may include the integration of noise filters, deployment on wearable platforms, and machine learning-based audio classification for improved accuracy.

## Declaration of conflict of interest

The authors have collectively contributed to the conceptualization, design, and execution of this paper. They have worked on drafting and critically revising the article to include significant intellectual content. This manuscript has not been previously submitted or reviewed by any other journal or publishing platform. Additionally, the authors do not have any affiliation with any organization that has a direct or indirect financial stake in the subject matter discussed in this manuscript.

## References

Alsalat, G.Y., El-Ramly, M., Fahmy, A.A. and Karim, S. (2018). Detection of mass panic using Internet of Things and machine learning. International Journal of Advanced Computer Science and Applications,9(5),320-329. doi: 10.14569/IJACSA.2018.090542

Ananthula, N., Rajeshwari, T., Mounika, B., Harsha-Vardhini, P.A. and Kalyani, B. (2022). Arduino based Rescue device with GPS Alert for Women Safety Application. International Mobile and Embedded Technology Conference (MECON), Noida, India, 343-347. doi:10.1109/MECON53876.2022.9751817.

Awodeyi, A.I., Moses, O., Makinde, O.S., Ben-Obaje, A.A. and Abayomi-Zannu, T.P. (2018). Design and Construction of a Panic Button Alarm System for Security Emergencies. International Journal of Engineering and Techniques, 4 (3), 649-652.doi:10.29126/23951303/IJET-V4I3P105.

Chandra, K. R., Nakka, T., Nadigatla, N., Reddy, V., Nulu, S. and Kali, A. (2023). Empowering Safety: Arduino-Based Alert System Design and Implementation for Women. 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 300-305.doi: 10.1109/ICECA58529.2023.10395065.

Damaševičius, R., Bacanin, N. and Misra, S. (2023). From Sensors to Safety: Internet of Emergency Services (IoES) for Emergency Response and Disaster Management. J. Sens. Actuator Net., 12(3),41. doi: 10.3390/jsan12030041

Fitriyan, R. and Syafii, S. (2024). Development design of an IoT-based smart home monitoring system with security features. Indonesian Journal of Electrical Engineering and Computer Science, 34(2), 788-794. doi: 10.11591/ijeecs.v34.i2.pp788-794

Jayanthi M., Mishra, I., Gowtham V., Poornima, R.M., Prakash, M. and Sneha, N.S. (2022). Arduino Based Women Safety Security System. EasyChair Preprint, 8304.

John H. L., Mahesh K. N., Navid S. (2017). Analysis of human scream and its impact on text-independent speaker verification. J. Acoust. Soc. Am. 141 (4), 2957–2967. doi: 10.1121/1.4979337.

Kalbande, M. Gaidhani, Y., Telrandhe, S. and Paul, M.C. (2023). Implementation of Smart Security Band for Women Safety. 5th International Conference on Smart Systems and Inventive Technology (ICSSIT),Tirunelveli,India,512-515. doi:10.1109/ICSSIT55814.2023.10061098.

Lazarou, I., Kesidis, A. L., Hloupis, G. and Tsatsaris, A. (2022). Panic detection using machine learning and real-time biometric and spatiotemporal data. ISPRS International Journal of Geo-Information, 11(11), 552. doi: 10.3390/ijgi11110552

Mohanty, S.; and Mishro, P. K. (2023). An IOT based Model for Monitoring Health Parameters using Arduino Mega. 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 1-5. doi:10.1109/ICCCNT56998.2023.10307347.

Nduka, A., Samual, J., Elango, S., Divakaran, S., Umar, U. and SenthilPrabha, R. (2019). Internet of Things Based Remote Health Monitoring System Using Arduino. Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 572-576. doi: 10.1109/I-SMAC47947.2019.9032438.

Ogunbiyi, D.T., Ogundoyin, I.K. and Akanbi. C.O. (2023a). A Context-Aware Human Distress Alert System for Safety from Interpersonal Violence using Smartphone Sensors. FUOYE Journal of Engineering and Technology (FUOYEJET), 8(1), 28-33. doi: 10.46792/fuoyejet.v8i1.997

Ogunbiyi, D., Ogundoyin, I., and Akanbi, C. (2023b). A Fuzzy Logic Model for Human Distress Detection. Journal of Engineering Studies and Research, 29(3), 49-56. doi: 10.29081/jesr.v29i3.005

Ruman, M.R., Barua, A., Rahman, W., Jahan, K.R., Jamil Roni, M. and Rahman, M.F.(2020). IoT Based Emergency HealthMonitoring System. International Conference on Industry 4.0 Technology (I4Tech),Pune,India,159-162. doi:10.1109/I4Tech48345.2020.9102647.

Sagar, R.H., Goud, L.K., Sharma, A., Ashraf, T. and Agrawal, A.P. (2022). Women Assault Detection and Providing Help Using Pitch, in Sugumaran, V., Upadhyay, D., Sharma, S. (eds) Advancements in Interdisciplinary Research. AIR 2022. Communications in Computer and Information Science.

Uwuigbe, O. (2017). The Viability of Screams as a Power Source. Journal of Interdisciplinary Science Topics, 4(2015), 1-3.

Venkatesh, K., Parthiban, S., Kumar, P.S. and Vinoth-Kumar C.N.S. (2021). IoT-based Unified approach for women's safety alert using GSM. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 388-392. doi: 10.1109/ICICV50876.2021.9388415.

Whitmore, A., Agarwal, A. and Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information systems frontiers, 17(1), 261-274.