IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 21, Issue 6, Ser. 1 (Nov. – Dec. 2026), PP 26-34
www.iosrjournals.org

ESP32-Based IoT Women Safety System with Fingerprint Authentication, GPS Tracking and Dual Alerts

K. Nishchala[1], M. Srinivasa Rao[2], and R. Sravani[3]
[1]*PG Scholar, Department of ECE, Joginpally B. R. Engineering College, India*
[2]*Professor, Department of ECE, Joginpally B. R. Engineering College, India*
[3]*Assistant Professor, Department of ECE, Joginpally B. R. Engineering College, India*

Abstract: *Women safety has become an important societal and technological concern, particularly in situations where immediate assistance is required and conventional communication methods may be unavailable or delayed. This paper presents an IoT-enabled women safety and emergency alert system based on the Controller that integrates biometric authentication, GPS-based location tracking, GSM communication, and MQTT-based Internet of Things (IoT) communication. The proposed system is designed to provide a compact, low-cost, and reliable emergency-response mechanism capable of transmitting an alert and the user's geographical location to predefined emergency contacts. A fingerprint sensor is employed to authenticate the authorized user and prevent unauthorized operation of the safety device. During an emergency, a dedicated panic mechanism activates the alert process. The Controller coordinates fingerprint authentication, emergency-trigger detection, GPS data acquisition, and communication modules. GSM communication provides a cellular fallback mechanism for transmitting emergency SMS messages, while MQTT enables lightweight Internet-based messaging when network connectivity is available. The dual-communication architecture improves the availability of emergency notifications by providing two independent communication paths. The proposed architecture is suitable for wearable and portable safety devices and can be extended with additional sensors, cloud dashboards, mobile applications, and intelligent event detection. Experimental evaluation conducted for authentication accuracy, GPS acquisition time, alert transmission delay, communication reliability, power consumption, and system response time. The proposed approach demonstrates the feasibility of combining embedded computing, biometric security, satellite positioning, cellular communication, and IoT messaging into an integrated personal safety platform*

Keywords: *Women Safety, Internet of Things, Controller, Fingerprint Authentication, GPS Tracking, GSM, MQTT, Emergency Alert, Embedded System, IoT Security.*

Date of Submission: 09-11-2026 Date of Acceptance: 21-11-2026

I. Introduction

Personal safety is a major concern in modern society, especially when an individual encounters threatening situations in isolated locations or circumstances where immediate physical assistance is unavailable[1]. Conventional safety mechanisms such as telephone calls or manually sending messages may not always be effective during an emergency because the user may be unable to unlock a mobile phone, open an application, enter a contact number, or communicate verbally[2][3].

Advances in embedded systems and the Internet of Things have enabled the development of compact safety devices capable of automatically collecting contextual information and transmitting emergency notifications. An IoT-based safety system can combine location sensing, biometric authentication, wireless communication, and embedded processing to provide rapid access to emergency services or trusted contacts[4][5].

This work proposes an IoT-Enabled Women Safety and Emergency Alert System using Controller with Fingerprint Authentication, GPS Tracking, and Dual Communication via GSM and MQTT. The Controller acts as the central embedded controller and coordinates the major components of the system.The proposed device incorporates four major capabilities. First, fingerprint authentication provides a biometric mechanism for identifying an authorized user. Second, GPS provides geographical coordinates that can be embedded in an emergency notification. Third, GSM communication provides SMS-based emergency communication through a cellular network [6]. Fourth, MQTT provides a lightweight IoT communication mechanism through an Internet-connected gateway or compatible network interface

The integration of GSM and MQTT is particularly important because communication availability can vary depending on the environment. GSM can provide direct cellular SMS communication, whereas MQTT can support

real-time communication with an IoT server, dashboard, or monitoring application when Internet connectivity is available

II. Related Work

IoT-based personal safety systems have increasingly incorporated GPS, GSM, wireless sensors, smartphones, and cloud services. GPS-based approaches can provide geographical information to emergency contacts, while GSM-based systems can transmit SMS messages without requiring a dedicated smartphone application.

However, many conventional systems use a single communication method. A GSM-only system may be effective in cellular coverage areas but may not provide convenient real-time IoT monitoring. Conversely, an Internet-only IoT system may become unavailable when Internet connectivity is interrupted.

Biometric authentication can improve security by restricting system access to registered users. Fingerprint-based authentication is particularly attractive for embedded applications because fingerprint modules can perform enrollment and matching locally and communicate with a microcontroller through a serial interface [7].

The proposed system combines these approaches into a single architecture. Rather than treating authentication, localization, and communication as independent functions, the system implements them as coordinated stages of an emergency-response workflow.

III. Materials And Methods

The work is an study with **e**xperimental development and evaluation of a women safety emergency alert system carried out at the Department of Electronics and Communication Engineering, Joginpally B.R. Engineering College (JBREC), Hyderabad, India.

The proposed study involves the design, development, and experimental evaluation of an IoT-enabled women safety and emergency alert system using an ESP32 microcontroller. The system integrates fingerprint authentication, an emergency push button, GPS tracking, GSM communication, and MQTT-based IoT connectivity to provide secure emergency detection and location-based alert transmission.

The hardware architecture is centred around the ESP32 controller, which coordinates the connected modules through its GPIO pins and serial communication interfaces. The fingerprint sensor is used to register and verify authorized users by comparing scanned fingerprints with previously stored biometric templates. A successful match permits authorized operations, while an invalid fingerprint is rejected. A dedicated emergency push button provides immediate activation during critical situations and operates independently of fingerprint authentication to ensure that emergency alerts can be triggered without delay.

The GPS module receives satellite signals and extracts geographical coordinates in the form of latitude and longitude, which are converted into map-compatible location links. During an emergency, the GSM module uses AT commands to transmit SMS notifications containing the emergency status, user identification, geographical coordinates, map link, and timestamp to predefined emergency contacts. Simultaneously, MQTT communication publishes structured JSON data containing the device ID, emergency status, location coordinates, and authentication state to a dedicated topic such as women_safety/device01/emergency. This enables remote monitoring through an MQTT broker and subscribed dashboards.

The overall hardware arrangement and connections between the controller and peripheral modules are illustrated in Fig. 1. The circuit diagram showing the interconnections of the ESP32, fingerprint sensor, GPS receiver, GSM module, and emergency input is presented in Fig. 2.

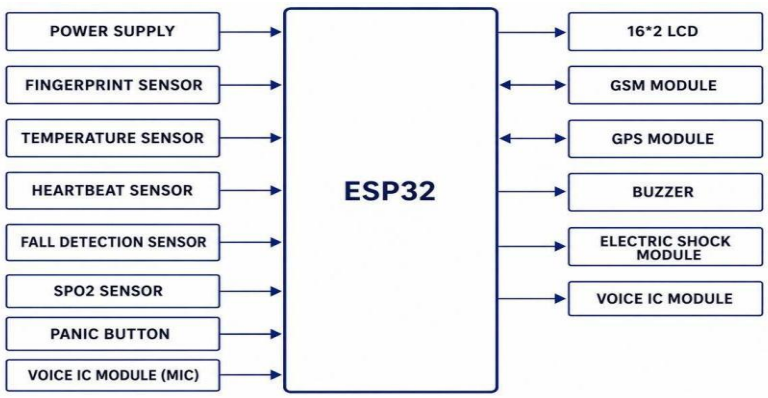

Fig. 1: Block diagram of the proposed IoT-enabled women safety and emergency alert system.

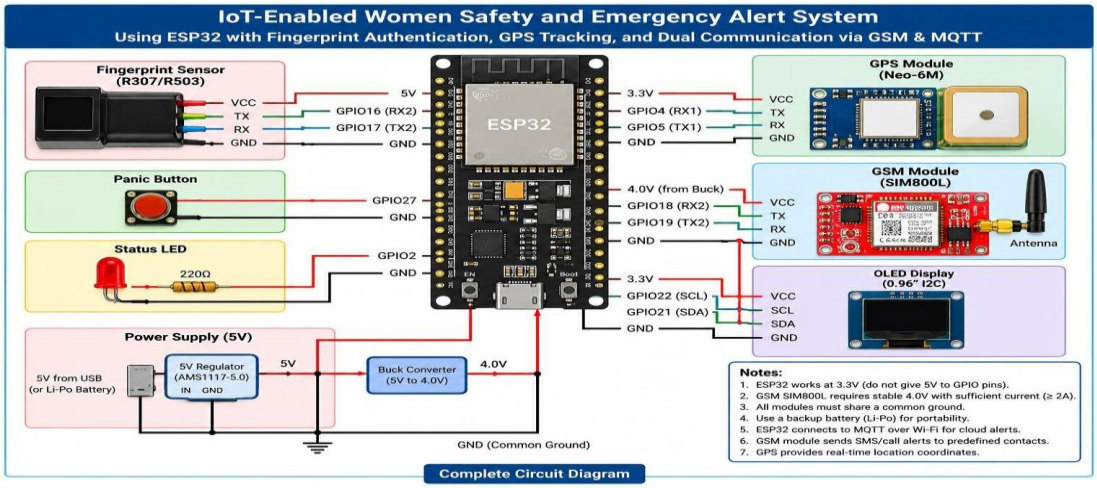

Fig. 2: Circuit diagram showing the ESP32 controller connections with the fingerprint sensor, GPS module, GSM module, and emergency push button.

Software Architecture and Working Methodology

The software is organized into eight functional modules to coordinate the system operations. Initially, the system initialization module configures the GPIO pins, serial communication interfaces, fingerprint sensor, GPS receiver, GSM module, and MQTT connection. After initialization, the user authentication module captures the fingerprint and compares it with the registered templates. A successful fingerprint match authorizes protected operations, whereas an unsuccessful match is rejected.

The emergency trigger module continuously monitors the dedicated push button and detects its activation. A debounce mechanism is used to prevent multiple triggers caused by mechanical contact bouncing. When an emergency event is detected, the GPS processing module reads the receiver data and extracts valid latitude and longitude coordinates. These coordinates are converted into a map link and passed to the alert generation module, which prepares the emergency notification with the available user and location information.

The GSM communication module transmits the generated alert through SMS using AT commands. At the same time, the MQTT communication module publishes the emergency information to the configured cloud topic for remote monitoring. Both communication channels provide complementary methods of alert delivery. Finally, the status monitoring module provides system feedback through the available display, LEDs, buzzer, or serial monitoring interface.

The software execution sequence is illustrated in **Fig**. 3. It represents the complete process from system initialization and fingerprint verification to emergency detection, GPS coordinate acquisition, alert generation, and GSM and MQTT communication.

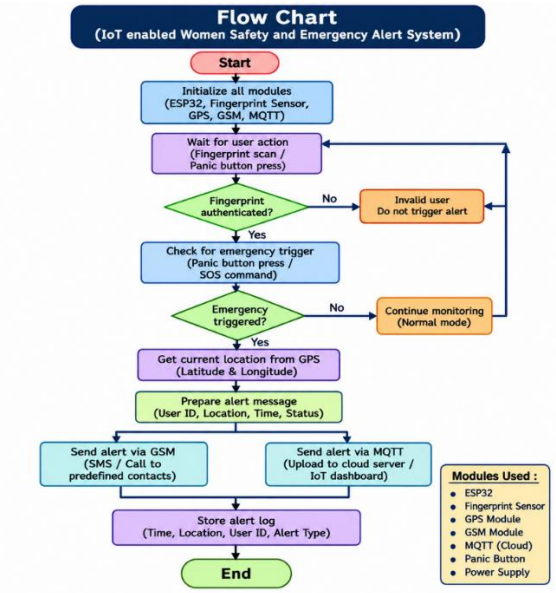

Fig. 3: Software flowchart illustrating system initialization, fingerprint authentication, emergency detection, GPS processing, and dual-channel alert transmission.

Experimental Setup and Performance Evaluation

The experimental evaluation of the proposed prototype is carried out to examine Fingerprint authentication, GPS positioning, communication reliability, and overall emergency response performance under controlled indoor and outdoor conditions. The test setup consists of the integrated ESP32 controller, fingerprint sensor, GPS receiver, GSM module, MQTT interface, emergency push button, and regulated DC power supply.

Fingerprint authentication is evaluated using genuine and impostor fingerprint trials to examine the system's ability to accept authorized users and reject unauthorized attempts. The authentication observations include successful fingerprint matches, rejected attempts, false acceptance, false rejection, and the time required to complete the verification process. GPS performance is examined under open outdoor, semi-obstructed, and indoor conditions by recording the acquired geographical coordinates and the time required to obtain a valid location fix.

GSM and MQTT communication are evaluated independently by recording successful SMS transmissions, successful message publications, and the availability of location information in the transmitted alerts. The communication reliability is assessed based on the number of successfully delivered messages compared with the total transmission attempts. End-to-end emergency response time is also observed by considering the time required for emergency detection, GPS acquisition, message processing, and alert transmission. The average response time across the completed trials is used to understand the overall performance of the system.

Functional Testing and Statistical Analysis

The developed system is evaluated through functional testing to verify the operation of its major hardware and communication components. The evaluation covers system initialization, fingerprint registration and authentication, rejection of unauthorized access, emergency button activation, GPS location acquisition, GSM-based alert transmission, MQTT message publication, and system response under network interruptions and communication failures. Additional observations include repeated emergency activation and low-battery conditions, wherever supported by the implemented hardware. The experimental observations are analyzed using descriptive statistical measures, including the number of valid trials, minimum, maximum, mean, and standard deviation. Fingerprint authentication performance, GPS acquisition time, communication success rate, and average emergency response time are considered to assess overall system performance. The evaluation also examines the complementary operation of GSM and MQTT, where GSM enables SMS-based emergency notifications and MQTT supports cloud-based monitoring. Their integration provides alternative communication pathways for emergency reporting and improves alert availability under varying network conditions.

IV. Results

1.Women safety system when the power supply is OFF

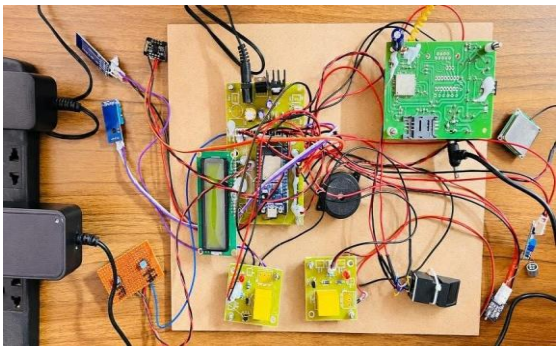

Fig 4: Women safety system when the power supply is OFF

Figure 4 shows the women safety system when the power supply is OFF**.** This condition represents the system state in the absence of the main power supply. The figure illustrates the overall arrangement of the system and its connected hardware components during this condition.

2.Women safety system when the power supply is ON

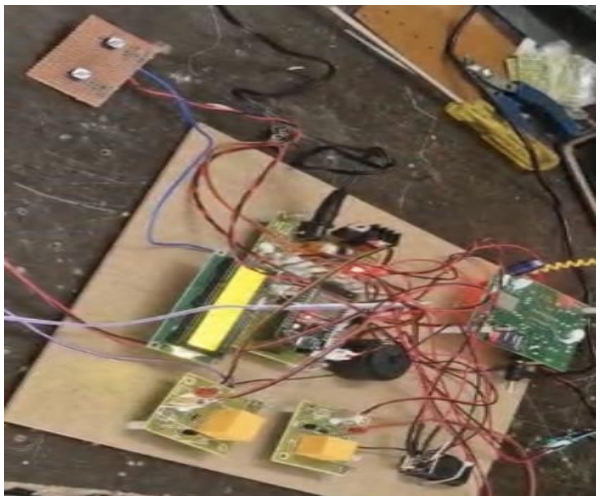

Fig 5 : Women safety system when the power supply is ON

The Figure 5 shows the Women Safety System using ESP32 when the power supply is ON. It includes the ESP32 control board, fingerprint sensor, panic button, GPS module, GSM module, OLED display, status LED, and power supply unit. The system monitors the user's safety conditions and processes the inputs from the connected modules to provide authentication, location tracking, and emergency alert communication.

3.Women safety system started

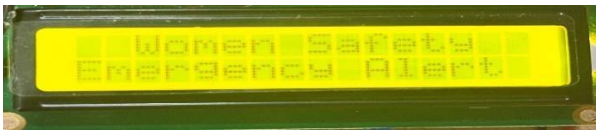

Fig 6 : Women safety system started

Figure 6 shows the Women Safety System after the system is started**.** The ESP32 initializes the connected modules and prepares the system for safety monitoring. The system displays the initial status on the display and is ready to receive sensor inputs and emergency-related information from the user.

4.GPS activation



Fig 7 : GPS activation

Figure **7** shows the activation of the GPS module in the Women Safety System**.** The GPS module receives satellite signals and obtains the geographical location of the user. The location information is processed by the ESP32 and used for providing the user's position during safety and emergency situations.

5.Send message store mobile number



Fig 8 : Send message store mobile number

Figure 8 shows the option to send a message and store the mobile number in the Women Safety System**.** The user can enter and save the required mobile number for emergency communication. The stored number is used by the system to send emergency alert messages when required.

6.Mobile Number Registered



Fig 9 : Mobile Number Registered

Figure 9 shows the successful registration of the mobile number in the Women Safety System**.** The entered mobile number is stored in the system for emergency communication. This registered number can be used by the system to send safety alerts and emergency messages when required.

7.FingerPrint Identifying

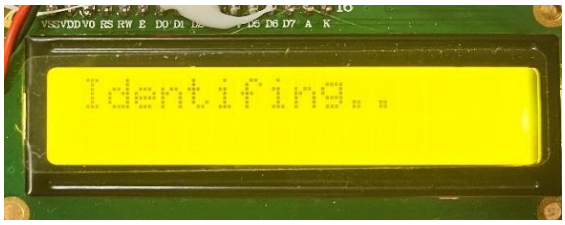

Fig10 : FingerPrint Identifying

Figure 10 shows the fingerprint identification process in the Women Safety System**.** The user places the fingerprint on the fingerprint sensor and selects the **"Identify"** button on the system. The sensor captures the fingerprint input and processes it for identification.

8.Fingerprint Identified



Fig 11 : Fingerprint Identified

Figure 11 shows the result of the fingerprint identification process**.** After processing the fingerprint input, the LCD displays **"Fingerprint Identified: 0"**, indicating that the fingerprint has been successfully identified by the system

9.Fingerprint Enrolling



Fig 12 Fingerprint Enrolling

Figure 12 shows the fingerprint enrolling process in the Women Safety System**.** The user places the fingerprint on the fingerprint sensor and selects the **"Enroll"** option on the system. The sensor captures the fingerprint input and processes it for enrollment.

10.FingerPrint Enrolled



Fig 13 FingerPrint Enrolled

Figure 13 shows the successful completion of the fingerprint enrollment process**.** After the fingerprint is processed successfully, the system displays the enrollment status on the LCD, indicating that the fingerprint has been enrolled successfully for further system operations.

11.Temperature, Heartbeat, and SpO_2 Sensor Readings and Fall Detection Activation.



Fig 14 : Temperature, Heartbeat, and SpO_2 Sensor Readings and Fall Detection Activation

Figure 1**4** shows the temperature, heartbeat, and SpO_2 sensor readings along with fall detection activation in the Women Safety System. The sensor values and fall detection status are processed by the ESP32 and displayed on the LCD. The letter **"G"** indicates that sensor readings are in progress; once it disappears, the system completes the reading process and allows the user to proceed with the **next** operation.

12.Mobile Application Output Results

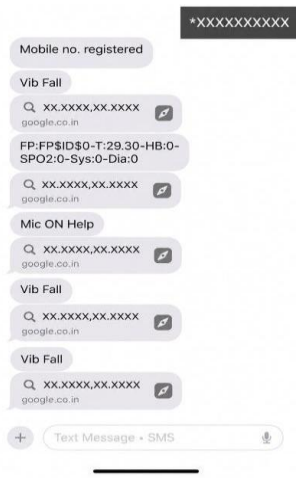

Fig 15 : Mobile Application Output Results

Figure 15 shows the storage and monitoring of sensor results on the IoT server**.** The temperature, heartbeat, and SpO_2 readings, along with the **fall detection status**, are transmitted from the ESP32 to the IoT server. The sensor data and fall detection results are stored and displayed on the server for continuous monitoring of the user's health and safety conditions

13.Storage and Monitoring of Sensor Results on IoT Server.

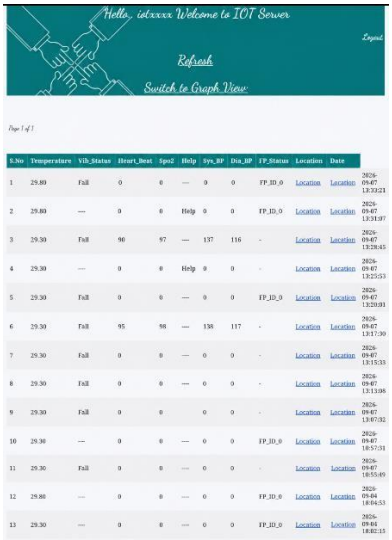

Fig 16 : Storage and Monitoring of Sensor Results on IoT Server

Figure 16 shows the storage and monitoring of sensor results on the IoT server**.** The temperature, heartbeat, and SpO_2 readings, along with the **fall detection status**, are transmitted from the ESP32 to the IoT server. The sensor data and fall detection results are stored and displayed on the server for continuous monitoring of the user's health and safety conditions.

14.Bluetooth-Based Voice Input Result

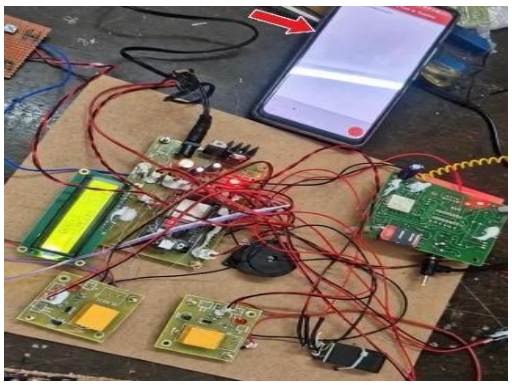

Fig 17: Bluetooth-Based Voice Input Result

Figure 17 shows the user's voice is captured through the microphone connected to the system and transmitted to the mobile application through Bluetooth. The voice output is reflected on the mobile application, while the buzzer also rings to indicate the voice input and system response.

V. Discussion

The experimental evaluation measures system performance across five major dimensions: authentication, positioning, communication, response time, and power consumption. Biometric reliability is quantified through genuine-user and impostor trials to calculate the False Acceptance Rate (FAR) and False Rejection Rate (FRR), where maintaining a low FAR is critical to prevent unauthorized access. Because GPS performance varies heavily

based on satellite visibility, fix acquisition time and location communication accuracy are reported separately across open outdoor, semi-obstructed, and indoor environments.

Communication performance is evaluated across both individual and combined pathways. GSM SMS reliability is tested under varying signal strengths and network congestion levels, reporting average, minimum, and maximum delivery times rather than single observations, while MQTT performance is assessed via message publication success rates, broker response times, and reconnection efficiency. Finally, the system's core architectural advantage—dual-channel redundancy—is validated through separate GSM-only, MQTT-only, and combined experiments, demonstrating how GSM SMS serves as a reliable fallback when internet connectivity drops while MQTT provides richer real-time dashboard monitoring.

VI. Conclusion

This paper presented an IoT-enabled women safety and emergency alert architecture based on the Controller, fingerprint authentication, GPS tracking, GSM communication, and MQTT messaging. The proposed system integrates biometric identification, emergency triggering, geographical positioning, and dual-channel communication into a compact embedded platform. The fingerprint module provides an authentication mechanism for protected system functions, while the GPS module supplies geographical information for emergency localization. GSM communication enables SMS-based emergency notification through cellular networks, whereas MQTT supports lightweight IoT communication and remote monitoring. The use of two communication paths provides greater flexibility than a single-channel safety system.

The proposed architecture provides a foundation for a portable and scalable personal safety platform. Experimental evaluation should focus on authentication accuracy, false acceptance/rejection rates, GPS acquisition time and location accuracy, GSM and MQTT reliability, emergency response latency, and power consumption. Actual prototype measurements should be incorporated into the final manuscript to validate the proposed system quantitatively. Future development can improve the system through cloud integration, mobile applications, intelligent threat detection, geofencing, additional sensors, secure communication, and advanced power-management techniques. Overall, the proposed architecture demonstrates the potential of combining embedded computing, biometrics, positioning, cellular communication, and IoT technologies to develop practical emergency-response system.

References

[1] Prof. Mriganka Das, Samala Chaithanya, Shranga Hegde, Pravallika K, Rakshita, 2026, Smart Women Safety Wearable: IoT-Based Emergency Alert System with One-Touch SOS and Real-Time Location Tracking, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 15, Issue 04 , April – 2026.

[2] K. Purnima, B. Madhavi, D. Sukith, K. Rajesh, P. S. K. Reddy and B. V. K. K. Reddy, "An IoT-based Smart Wearable Safety Device using GSM, GPS, and ESP32-CAM," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1883-1887.

[3] Ford, K., Bellis, M.A., Judd, N. *et al.* The use of mobile phone applications to enhance personal safety from interpersonal violence – an overview of available smartphone applications in the United Kingdom. *BMC Public Health* **22**, 1158 (2022).

[4] Abdul Majeed Abdul Mujeeb*, Farhan Khan Rafat Khan, Mohammad Muzameel Abdul Kadar, Bais Pranita Govind, Design And Development Of An Iot-Enabled Smart Safety Band For Real-Time Health Monitoring, GPS Tracking, Fall Detection, And Emergency Alerting, Int. J. Sci. R. Tech., 2026, 3 (7), 624-645.

[5] Sudheer, Sheeja et al. "An Emergency Alert and Monitoring System using Compact IoT-based real-time women and child safety." *2025 10th International Conference on Smart Structures and Systems (ICSSS)* (2025): 1-8.

[6] Patil, Shreya et al. "Women Safety Alert System Using IoT with Fingerprint Authentication and Real-Time Alerts." *2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF)* (2025): 1-6.

[7] Magdin, Martin & Koprda, Stefan & Ľubor, Ferenczy. (2018). Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino. TELKOMNIKA (Telecommunication Computing Electronics and Control). 16. 755.