Journal of Mechatronics Engineering

Prevention of Violence Against Women: Proof of Concept of a Wearable Device for Everyday Risk Monitoring

INÁCIO LIMA DE SOUZA FILHO[1], MARIA VITÓRIA DE FREITAS GOMES[1], JERMANA LOPES DE MORAES[1]

[1]Department of Computer Engineering, Federal University of Ceará (UFC), Sobral Campus, Sobral, CE, Brazil
<inaciofilhoufc@alu.ufc.br>

DOI: 10.21439/jme.v9i1.141

Abstract. Everyday violence against women is a serious social problem that demands innovative solutions. This work presents a proof of concept of a wearable device for women's safety, integrating embedded systems, wireless communication, and geolocation. The device uses the ESP32 microcontroller running FreeRTOS (*Free Real-Time Operating System*) firmware and connects GPS (*Global Positioning System*), accelerometer, gyroscope, and digital microphone sensors for real-time risk detection. The architecture comprises sensor data collection, local processing by the ESP32, a Node.js *back-end*, a MongoDB database, and a React *front-end* for visualization and control. Results demonstrate the technical feasibility of integrating multiple sensors into an alert system capable of detecting suspicious movements, capturing audio evidence, and tracking location in real time. The proof of concept combines automatic detection with manual triggering, broadening the functionalities compared to previous solutions. The physical prototype was developed using a custom printed circuit board manufactured at the Federal University of Ceará, Sobral Campus Laboratory. Improvements in miniaturization, energy optimization, and real-world validation are still required before commercial viability. This research is expected to serve as a starting point for initiatives aimed at reducing violence against women, demonstrating the potential of technology in promoting women's safety and autonomy.

Keywords: Violence against women. Wearable technologies. Internet of Things. ESP32. Personal safety.

(Received May 13th, 2026 / Accepted June 10th, 2026)

1 Introduction

Technological progress presents significant opportunities to address critical security issues, especially those faced by vulnerable groups in society. Women, for example, face significant risks in their daily lives, including harassment, physical violence, and psychological abuse. Global statistics indicate that one in three women has experienced some form of violence in their lifetime, highlighting the seriousness and scope of this problem. Specifically in Brazil, the rates of violence against women are alarming, demonstrating the urgent need for measures aimed at protecting and ensuring their safety (GARCÍA-MORENO et al., 2013). In this context, the use of emerging technologies has proven to be a promising strategy for reducing or preventing these problems and promoting personal security (KOUZANI, 2023).

The use of wearable devices presents itself as a potential alternative, both for monitoring the safety of users and as a tool to alert authorities and/or family members about risky situations in order to obtain immediate assistance. These devices can integrate motion sensors, geolocation, and wireless communication, providing continuous and discreet monitoring of the user's safety (PATEL; HASAN, 2018).

The automation of personal protection mechanisms is increasingly discussed in the literature. We can highlight the work of Viswanath *et al.* (2016) that integrated acceleration sensors into footwear, enabling the identification of fall events and data transmission via Bluetooth, achieving a classification accuracy of 97.5% (VISWANATH; PAKYALA; MUNEESWARI, 2016). Meanwhile, Hyndavi *et al.* (2020) developed an autonomous sensor array with GSM (*Global System for Mobile Communications*) connectivity, combining pressure, temperature, and biometric tracking to verify an individual's physiological responses (HYNDAVI; NIKHITA; RAKESH, 2020). Additionally, Patel and Hasan (2018) implemented machine learning algorithms in a bracelet disguised as jewelry to detect sudden movements, typical fall patterns, or an assault (PATEL; HASAN, 2018). More recently, Wagh *et al.* (2025) embedded machine learning in a wearable device to autonomously classify distress situations from multisensor data, reinforcing the shift toward automated detection (WAGH et al., 2025).

Although wearable devices for monitoring individuals are widely used in the literature, they exhibit critical functional gaps. Systems relying exclusively on manual push-buttons fail during surprise attacks (PATEL; HASAN, 2018; VISWANATH; PAKYALA; MUNEESWARI, 2016). Conversely, autonomous systems often introduce severe power consumption penalties and complex physical footprints that hinder practical deployment (GHOSH et al., 2021). Therefore, we recognize a need for a hardware architecture that balances automatic emergency detection with energy consumption limitations.

The objective of this work is the development of a proof of concept of a wearable device designed to automate safety alerts for women. We engineered a system integrating an ESP32 processing core, I2S (*Inter-IC Sound*) digital audio capture, I2C (*Inter-Integrated Circuit*) kinematic tracking, and GPS (*Global Positioning System*) polling over UART (*Universal Asynchronous Receiver-Transmitter*) (SYSTEMS, 2024). The prototype acts strictly as a feasibility benchmark. We explicitly acknowledge that the current iteration faces severe constraints regarding component miniaturization, identifying the specific hardware limitations that future iterations must address (HYNDAVI; NIKHITA; RAKESH, 2020; PENCHALAIAH et al., 2021).

2 Related Works

The growing incidence of violence against women has driven a rapid expansion of technological countermeasures, and recent systematic reviews confirm the accelerated maturation of this field. In the specific domain of IoT for personal safety, Farooq *et al.* (2023) (FAROOQ et al., 2023) surveyed IoT-based women safety solutions, classifying the sensors, machine learning algorithms, and embedded wearables most frequently adopted. From the standpoint of wearable hardware, Dian *et al.* (2020) (DIAN; VAHIDNIA; RAHMATI, 2020) surveyed the opportunities and challenges of integrating wearables with the IoT, emphasizing the constraints of energy consumption and miniaturization that still limit such devices. Regarding automatic risk detection, Zhang *et al.* (2022) (ZHANG et al., 2022) reviewed deep learning advances for human activity recognition with wearable sensors, which increasingly favor automatically learned representations over hand-crafted features. Finally, in the context of intelligent monitoring systems, Bhuvaneswari and Thangamuthu (2025) (BHUVANESWARI; THANGAMUTHU, 2025) reviewed assault detection technologies, highlighting the convergence of artificial intelligence, IoT, and wearables toward automated emergency response. Together, these works delimit the state of the art against which the device-level proposals discussed next are positioned.

Recent hardware developments have attempted to transition personal security mechanisms from manual triggers to automated sensor networks. Patel and Hasan (2018) (PATEL; HASAN, 2018) designed a smart bracelet built on an Adafruit Flora (Arduino-compatible) controller, integrating a heterogeneous sensor suite that includes accelerometer, gyroscope, temperature, pressure, GPS, and microphone. The device uses embedded sensors and machine learning algorithms to automatically identify movement patterns associated with risky situations, such as falls, physical assaults, or unusual sudden movements, then transmits GPS coordinates to emergency responders. The architecture, however, relies entirely on a smartphone as a secondary relay for placing 911 calls and dispatching SMS (*Short Message Service*) alerts, creating a single point of failure during active physical assault scenarios.

Hyndavi *et al.* (2020) (HYNDAVI; NIKHITA; RAKESH, 2020) proposed an Arduino-Uno-based device that combines pressure, temperature, and pulse-rate sensors with a dedicated push button, integrating a SIM808 module for combined GPS positioning and GSM connectivity. The proposal employs both an automatic mechanism, triggered when sensor thresholds indicate a critical situation, and a manual mechanism, activated by the user when she feels unsafe. Upon either trigger, the device sends the real-time GPS location through an SMS containing a Google Maps link to pre-registered contacts. Although it eliminated dependence on smartphones, the system exhibited excessive false positive rates due to non-deterministic biometric thresholds, and ambient signal attenuation further degraded the reliability of GSM transmissions.

Ghosh *et al.* (2021) (GHOSH et al., 2021) implemented a Raspberry-Pi-Zero-based evidence capture system integrating a flex sensor (used as the activation trigger), an IR sensor, a camera, a microphone for audio capture, and a SIM808 module providing combined GPS positioning and GSM connectivity. The system continuously transmits the victim's location and uploads captured images, video, and audio to a remote web server as evidence. However, the physical limitations of the microprocessor imposed prohibitive power consumption penalties, requiring a battery with dimensions incompatible with use in wearable devices. These limitations dictate the need to transition to ultra-low power microcontrollers, such as the ESP32, to meet the thermal and current limits of continuous monitoring in wearable devices.

In contrast, Viswanath *et al.* (2016) (VISWANATH; PAKYALA; MUNEESWARI, 2016) developed a footwear-mounted device based on a Light Blue Bean board (ATmega328P, Arduino-compatible), using a BMA250 tri-axial accelerometer as the sole on-device sensor to identify a deliberate foot-tap gesture as the activation pattern. Upon detecting the tap sequence, the wearable communicates via Bluetooth Low Energy (BLE) with the user's paired smartphone, which then dispatches SMS alerts containing the location to pre-registered contacts. The approach eliminates the need for a manual button, but the device itself contains no GPS or GSM module, inheriting a critical dependency on the smartphone for both communication and location resolution.

More recently, Wagh *et al.* (2025) (WAGH et al., 2025) proposed an IoT wearable that replaces fixed thresholds with machine learning. The device fuses physiological sensors (heart rate and temperature) with kinematic and positioning sensors (accelerometer and GPS) and employs a hybrid classifier combining Support Vector Machine, Naive Bayes, and convolutional networks to recognize distress situations, offering both automatic detection and a manual push-button trigger and reporting up to 99.7% accuracy before transmitting the GPS coordinates over GSM. Although the multimodal machine learning approach reduces false alarms relative to single-sensor thresholds, the architecture still relies on GSM messaging as its sole notification channel and does not record ambient audio as evidence.

Islam *et al.* (2019) (ISLAM et al., 2019) implemented a low-cost device based on a PIC16F887A microcontroller, combining a GPS module with three dedicated push buttons that let the user categorize the type of emergency before dispatching an SMS with her real-time location through a GSM module to predefined contacts. Although robust in its location-tracking function, the system depends entirely on manual activation, rendering it ineffective when the victim is incapacitated, and its through-hole construction powered by four AA cells is incompatible with discreet wearable use.

Zikriya *et al.* (2018) (ZIKRIYA et al., 2018) developed a smart pendant built around a NodeMCU ESP-12E Wi-Fi module and an ultrasonic sensor that, by estimating the proximity of an aggressor, acts as an automatic trigger, combined with an LED flash intended to disorient the attacker and emergency calls dispatched through the Twilio cloud service; a companion Raspberry Pi unit captures the attacker's image and the victim's location. The automatic proximity-based activation removes the need for manual input, but relying on ultrasonic distance thresholds tends to produce frequent false positives during ordinary daily activities, while the cloud-dependent alerting adds latency that is critical in emergency scenarios.

The vast majority of the aforementioned prototypes fail to balance operational autonomy with hardware efficiency. Implementations either rely on manual activation to trigger alerts, rendering them ineffective in situations where the victim is incapacitated, or they exhibit high energy consumption, a significant limitation for embedded systems (GHOSH et al., 2021; PATEL; HASAN, 2018). Furthermore, biomedical sensors or devices installed in areas such as the feet tend to generate frequent false positives during routine physical activities or everyday movements (HYNDAVI; NIKHITA; RAKESH, 2020). Consequently, a device that reduces these limitations, operating with multiple sensors and with reduced energy consumption, remains a challenge for the development of low-cost wearable devices.

Table 1 maps the main technologies and architecture used in the aforementioned works, comparing them with the present proposal. As a key differentiator, our proof of concept of a wearable device projects a hybrid acquisition layer. By simultaneously querying acceleration sensors (I2C) and transmitting raw I2S digital audio, the ESP32 firmware merges deterministic threshold algorithms with active telemetry. This archi-

Table 1: Architectural comparison of proposed proof of concept of a wearable device against related personal safety systems.

Feature	Patel (PATEL; HASAN, 2018)	Viswanath (VISWANATH; PAKYALA; MUNEESWARI, 2016)	Hyndavi (HYNDAVI; NIKHITA; RAKESH, 2020)	Ghosh (GHOSH et al., 2021)	Wagh (WAGH et al., 2025)	Islam (ISLAM et al., 2019)	Zikriya (ZIKRIYA et al., 2018)	This Work
Auto Detection	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Manual Trigger	No	No	Yes	No	Yes	Yes	No	Yes
Audio Capture	Yes	No	No	Yes	No	No	No	Yes
GPS Tracking	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Real-time Dashboard	No	No	No	No	No	No	No	Yes
Open-source code	No	No	No	No	No	No	No	Yes
Microcontroller	Adafruit Flora	Arduino	Arduino Uno	Rasp. Pi	Arduino/RPi	PIC	NodeMCU	ESP32
Multiple sensors	Yes	No	Yes	Yes	Yes	No	Yes	Yes

tecture surpasses the logic of isolated sensors, merging real-time GPS tracking, dual trigger mechanisms, and HTTP (*HyperText Transfer Protocol*) data logging into a unified open-source stack made available via GitHub. Note that the proposed prototype integrates all the technologies presented in Table 1, unlike other works, which are usually limited to the isolated use of only one approach or specific set of solutions.

3 System Context and Hardware Motivation

To overcome many of the limitations listed in the previous section, we developed a proof of concept of a wearable device designed to automate distress signaling without user interaction. The hardware architecture utilizes an ESP32 microcontroller as the central processing node. In addition, it integrates a GY-NEO7M GPS module for coordinate tracking, an MPU-6050 for detecting sudden movement anomalies, and an SPH0645LM4H digital microphone via I2S for capturing raw ambient audio. A brief description of the components used follows.

3.1 ESP32

The ESP32 microcontroller, developed by Espressif Systems, has become prominent in the development of IoT (*Internet of Things*) applications. These devices offer integrated Wi-Fi connectivity, low power consumption, and a high level of performance, making them ideal for projects that require wireless communication and efficient processing (GHOSH et al., 2021). Fig. 1 shows one of the board models, ESP32-WROOM-32, which was used in this work.

This platform features robust technical characteristics for IoT applications. The device has a dual-core Xtensa® 32-bit LX6 processor operating at up to 240 MHz, offering high processing power. It has 520 KB of internal SRAM and supports external flash memory of up to 16 MB, providing ample space for code and data storage. The module offers Wi-Fi connectivity in the 802.11 b/g/n standards and *Bluetooth* v4.2 BR/EDR and BLE, enabling multiple forms of wireless communica-

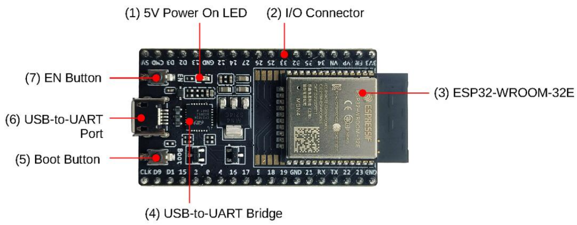

Figure 1: ESP32-DevKitC V4 with the ESP32-WROOM-32 module. (SYSTEMS, 2024).

tion. It features 34 programmable GPIO (*General Purpose Input/Output*) pins, which can be configured for various functions, including 18 12-bit ADC (*Analog-to-Digital Converter*) channels, 2 8-bit DAC (*Digital-to-Analog Converter*) channels, UART, SPI (*Serial Peripheral Interface*), and I2C interfaces for peripheral communication, as well as PWM (*Pulse Width Modulation*) support for device control on all pins (SYSTEMS, 2024).

The ESP32 also integrates security features such as *hardware* encryption, making it suitable for applications that require data protection (HYNDAVI; NIKHITA; RAKESH, 2020). Fig. 2 illustrates the internal diagram of the ESP32, showing the organization of these components and modules, as well as the high level of integration of the microcontroller, which concentrates multiple functionalities in a single embedded platform.

3.2 Geolocation and GPS

The integration of geolocation functionalities in personal security devices is fundamental for real-time monitoring of emergency situations (HYNDAVI; NIKHITA; RAKESH, 2020).

For this functionality and in this work, the GY-NEO7M module was used, based on the u-blox NEO-7M GPS *chipset*, which stands out for its high signal sensitivity, capability of tracking up to 22 satellites simultaneously, and fast position acquisition, or TTFF (*Time To First Fix*). This parameter refers to the time

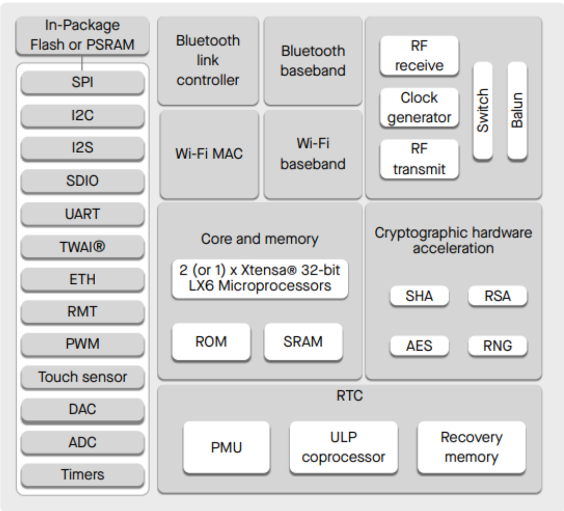

Figure 2: Internal diagram of the ESP32. Source: (SYSTEMS, 2024).

interval that the GPS module requires to acquire sufficient signals from satellites and determine the first valid position after being activated, which is crucial for applications where speed in obtaining location is necessary (KASHALKAR, 2021). The module can operate at voltages from 3.3 V to 5 V and communicate via UART. The module is shown in Fig. 3.

3.3 Microphone

The use of microphones in personal security devices allows for the detection of sounds or keywords associated with risky situations, as well as assisting in environmental analysis and the capture of auditory evidence in cases of violence (MURALEEDHARAN; GARCIA-CONSTANTINO, 2022). The digital microphone model used in this work is SPH0645LM4H, illustrated in Fig. 4, which presents suitable characteristics for applications in wearable security devices. This sensor is a MEMS (*Micro-Electro-Mechanical Systems*) microphone with I2S digital output, which allows efficient integration with microcontrollers such as the ESP32, eliminating the need for external analog-to-digital converters.

3.4 Accelerometer

The accelerometer is another relevant component in personal security devices, as it allows the detection of

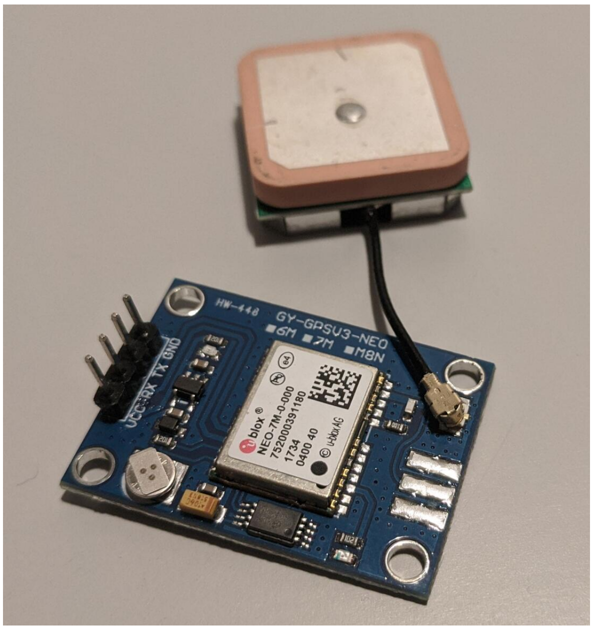

Figure 3: GY-NEO7M geolocation module used. Source: (KASHALKAR, 2021).

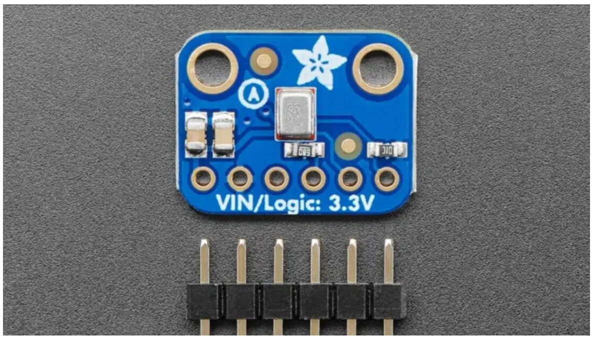

Figure 4: SPH0645LM4H Digital Microphone Module used in this project. Source: (HWLibre, 2024).

variations in movement and inclination of the device across three standardized axes (x, y, and z). This makes it possible to identify situations such as falls, sudden movements, or even the use of physical force against the user (HYNDAVI; NIKHITA; RAKESH, 2020). The reliability of such motion-based detection has advanced considerably with deep learning, as consolidated by a recent review on wearable human activity recognition (ZHANG et al., 2022), which progressively favors automatically learned representations over hand-crafted features.

The accelerometer module used in this work is the MPU-6050, illustrated in Fig. 5, which is widely used in applications that require precise measurement of motion and orientation. This sensor combines an accelerometer and a 3-axis gyroscope in a single *chip*, enabling the simultaneous detection of linear acceleration and angular velocity. For communication with the ESP32, the MPU-6050 uses the I2C protocol (HYNDAVI; NIKHITA; RAKESH, 2020), simplifying the system architecture by reducing the number of required connections and ensuring efficient communication between components (PENCHALAIAH et al., 2021).

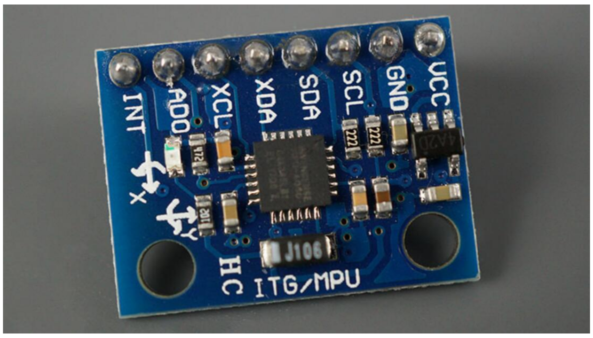

Figure 5: MPU-6050 Accelerometer and Gyroscope Module. Source: (HWLibre, 2024).

In embedded systems, the MPU-6050 can be integrated to continuously monitor movement behavior. If an abnormal acceleration pattern or fall is identified, the system can trigger an automatic alert with real-time location, assisting in the rapid activation of emergency contacts (PENCHALAIAH et al., 2021).

The adoption of accelerometers in personal security solutions therefore represents a strategy for risk prevention and mitigation, broadening the range of functionalities of alert devices and enabling a more robust response to physical threats (HYNDAVI; NIKHITA; RAKESH, 2020; PENCHALAIAH et al., 2021).

4 Methodology

This section details the methodology applied to develop the proof of concept of a wearable device proposed here. The system architecture encompasses the sensor data acquisition layer via ESP32, the fabrication of the physical prototype, and the associated data transmission infrastructure (back-end, database, and front-end). Fig. 6 illustrates the system data flow.

4.1 Stage 1: Data Collection

In the first stage of the methodology, the ESP32 development board was used to collect data from the GPS, accelerometer, microphone, and emergency button sensors incorporated into the proof of concept of this work. The schematic diagram of the connections of these elements is presented in Fig. 7.

Individual functionality tests were conducted for each module before system integration. Initially, the GPS was configured and tested for coordinate accuracy and signal acquisition time. Next, the MPU-6050 (accelerometer and gyroscope) was calibrated and evaluated for abnormal event detection, while the SPH0645LM4H digital microphone had its audio capture and transmission verified. After isolated validation, progressive integration of the components was performed, enabling the identification and correction of potential interferences between subsystems.

Additionally, the calibration of the MPU-6050 accelerometer and gyroscope involved determining the *offset* values on the three axes (x, y, z) with the device at rest, allowing compensation of systematic deviations in acceleration and rotation measurements.

The collected data were processed locally by the ESP32 to identify significant events, such as emergency button activations or detection of suspicious movements. After initial processing, this information was prepared and sent to the *back-end* through secure HTTP communication protocols, ensuring the integrity and confidentiality of the transmitted data.

4.1.1 Firmware Architecture

The *firmware* in the ESP32 was developed using the FreeRTOS (*Free Real-Time Operating System*), which enables efficient management of multiple concurrent tasks. The *firmware* architecture was organized into independent *tasks*, each responsible for a specific subsystem of the device, enabling parallel execution and functionality isolation.

The main implemented *tasks* were:

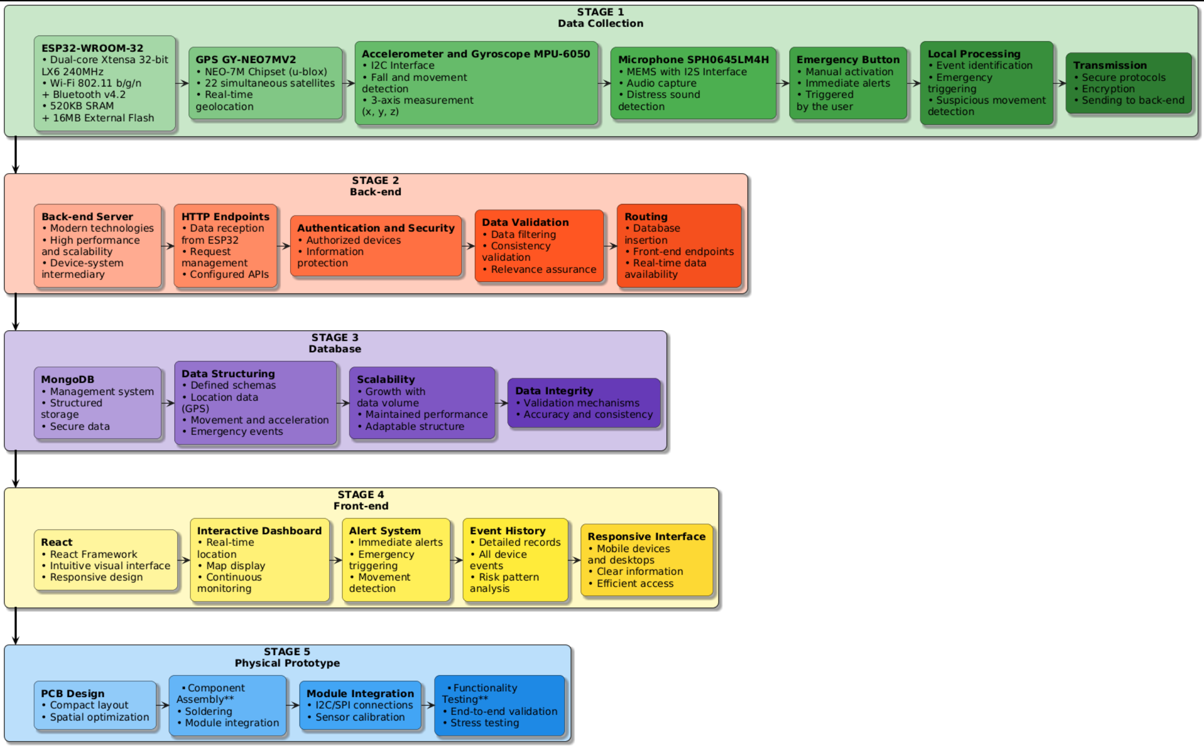

Figure 6: System architecture and data flow diagram. Source: Author.

- GPS *Task*: responsible for periodic reading of location coordinates, with an update interval configured to 5 seconds;
- Accelerometer/Gyroscope *Task*: continuously monitors motion data from the MPU-6050 sensor, applying an abnormal event detection threshold based on total acceleration ($totalG < 0.25$ or $totalG > 6.0$), where values outside this range indicate possible falls or sudden movements;
- Microphone *Task*: performs continuous audio capture through the SPH0645LM4H digital microphone, sending data packets every 1 second to the *back-end*;
- Communication *Task*: manages the transmission of collected data to the server via HTTP requests.

The device's Internet connectivity is established through a Wi-Fi connection, requiring the user to share the mobile data network from her *smartphone* (*hotspot* function). This approach was adopted considering that the ESP32 does not have an integrated cellular communication module, and the use of the phone's *hotspot* represents a practical and low-cost solution to ensure device connectivity in outdoor environments.

4.2 Stage 2: Back-end

The *back-end* system was configured to manage all requests received from the ESP32, process the data, and route them appropriately to the database or to the *front-end*. Additionally, it was structured to allow future expansions and integrations with other systems, ensuring flexibility and adaptability to the project's needs.

The main functionalities implemented in the back-end included the configuration of HTTP endpoints for receiving data sent by the ESP32, as well as the implementation of authentication and encryption mechanisms, ensuring that only authorized devices could transmit information securely. Data filtering and validation routines were also developed, ensuring data consistency. Regarding audio processing, the packets received every second are accumulated until completing 17 seconds, at which point they are converted into MP3

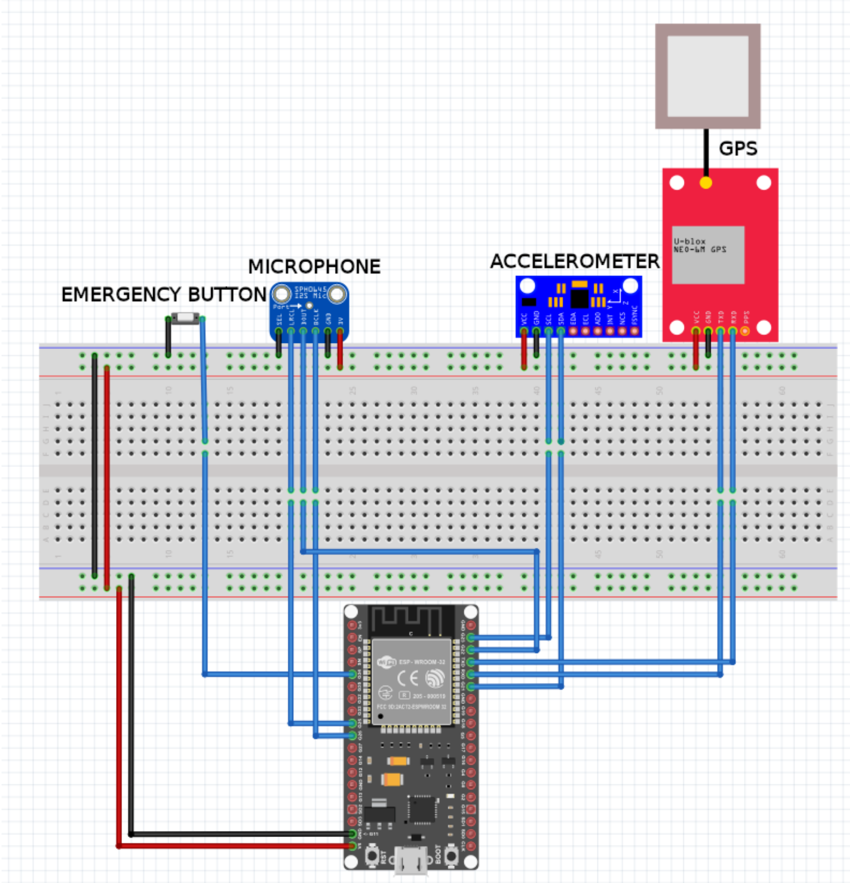

Figure 7: Hardware schematic detailing ESP32 sensor interfacing. Source: Author.

format files, optimizing storage and facilitating playback. Finally, functions were created for inserting data into the database and providing endpoints for real-time access by the front-end.

4.2.1 Privacy and Data Security

The privacy and security of data collected by the proof of concept of a wearable device were treated as fundamental system requirements, considering the sensitivity of user location and emergency information. To ensure adequate data protection, two main security mechanisms were implemented: JWT (*JSON Web Token*) authentication and encrypted communication via the HTTPS (*HyperText Transfer Protocol Secure*) protocol.

JWT was used as an authentication and authorization mechanism between the ESP32 device and the *back-end*. Each device receives a unique *token* at the time of registration, which must be included in the header of all HTTP requests sent to the server. The JWT is composed of three parts: *header*, *payload*, and *signature*. The signature is generated using the HMAC SHA-256 algorithm with a secret key stored exclusively on the server, ensuring that only tokens generated by the system are accepted. Thus, requests from unauthorized devices or with tampered *tokens* are automatically rejected by the *back-end*.

For data-in-transit protection, all communication between the proof of concept of a wearable device and the server was performed using the HTTPS protocol. HTTPS uses TLS (*Transport Layer Security*) encryption to establish a secure communication channel, preventing third parties from intercepting or modifying transmitted data. As a result, sensitive information such as location coordinates, emergency data, and audio recordings are encrypted before being sent over the network, making them unreadable to potential attackers who might attempt to intercept the communication.

4.3 Stage 3: Database

The database was implemented to store all information collected by the proof of concept of a wearable device in a structured and secure manner. MongoDB was used as the database management system, considering the specific performance and scalability needs identified during development.

The database implementation included the definition of schemas that organized location, movement, and emergency event data efficiently. The structure was designed to support the growth in data volume generated by the proof of concept of a wearable device without compromising system performance. Additionally, validation mechanisms and *constraints* were used to ensure that stored data were accurate and consistent, guaranteeing information integrity over time.

4.4 Stage 4: Front-end

The *front-end* was developed for mobile devices and desktops, using the React framework, providing an intuitive and responsive user experience. Among the implemented functionalities, the interactive *dashboard* stands out, displaying the real-time location of users on a map, enabling continuous monitoring of the situation. An alert system was also implemented that presents immediate notifications in case of emergency button activation or detection of suspicious movements, allowing rapid responses to risk situations. Additionally, an event history functionality was developed that provides a detailed record of all occurrences captured by the proof of concept of a wearable device, facilitating subsequent analyses and identification of risk patterns.

4.5 Stage 5: Physical Prototype

To validate the hardware integration, we fabricated a custom Printed Circuit Board (PCB). We designed the layout with 1 mm track widths to support current surges, maintaining a 0.2 mm clearance to mitigate crosstalk between the I2S and I2C buses. The board was milled via a CNC (*Computer Numerical Control*) machine.

The power supply architecture utilizes two 18650 lithium-ion cells in series, delivering a nominal 7.4 V with a 3600 mAh capacity. Empirical power profiling revealed a continuous current draw of 360 mA during the active monitoring state (continuous Wi-Fi transmission and sensor polling). This current load is excessively high for a wearable application, fundamentally restricting the device's operational autonomy.

5 Hardware and System Results

This section documents the empirical results derived from the physical prototype. We evaluated the hardware integration, power profile, and back-end telemetry latency under simulated stress conditions, following standard experimental procedures for IoT-based safety systems (HYNDAVI; NIKHITA; RAKESH, 2020). Source code for the tested firmware and back-end services is maintained in the project repository[1].

5.1 Sensor Data Acquisition and Telemetry

During active polling, the ESP32 successfully established I2C communication with the MPU-6050 and UART communication with the GY-NEO7M, maintaining data integrity across the various hardware buses (SYSTEMS, 2024). Fig. 8 logs the telemetry sequence, confirming the extraction of x, y, and z kinematic vectors alongside geospatial coordinates. The system successfully resolved location data and streamed the calculated $totalG$ values to the serial interface for debugging, satisfying the requirements for real-time tracking established in previous studies (KASHALKAR, 2021).

```
GPS:   Lat: -3.693204 | Lon: -40.354280 | Satellites: 8
Accel: X: +0.12 g | Y: -0.08 g | Z: +0.98 g
Gyro:  X: +1.24 °/s | Y: -0.56 °/s | Z: +0.32 °/s
--------------------------------------------------
GPS:   Lat: -3.693204 | Lon: -40.354280 | Satellites: 8
Accel: X: +0.14 g | Y: -0.06 g | Z: +0.97 g
Gyro:  X: +1.12 °/s | Y: -0.48 °/s | Z: +0.28 °/s
--------------------------------------------------
GPS:   Lat: -3.693205 | Lon: -40.354281 | Satellites: 9
Accel: X: +0.10 g | Y: -0.09 g | Z: +0.99 g
Gyro:  X: +0.98 °/s | Y: -0.62 °/s | Z: +0.18 °/s
--------------------------------------------------
GPS:   Lat: -3.693205 | Lon: -40.354281 | Satellites: 9
Accel: X: +0.11 g | Y: -0.07 g | Z: +0.98 g
Gyro:  X: +1.05 °/s | Y: -0.52 °/s | Z: +0.22 °/s
--------------------------------------------------
GPS:   Lat: -3.693206 | Lon: -40.354282 | Satellites: 9
Accel: X: +0.13 g | Y: -0.05 g | Z: +0.97 g
Gyro:  X: +1.18 °/s | Y: -0.44 °/s | Z: +0.30 °/s
--------------------------------------------------
```

Figure 8: Serial output detailing coordinate acquisition and kinematic vector polling. Source: Author.

[1] Available at: <https://github.com/inaciolimaf/TCC>

The I2S interface bypassed analog conversion, feeding raw digital audio from the SPH0645LM4H directly to the microcontroller buffer. The data was packetized and transmitted via Wi-Fi (Fig. 9), ensuring the preservation of auditory evidence as proposed in multi-sensor safety architectures (MURALEEDHARAN; GARCIA-CONSTANTINO, 2022).

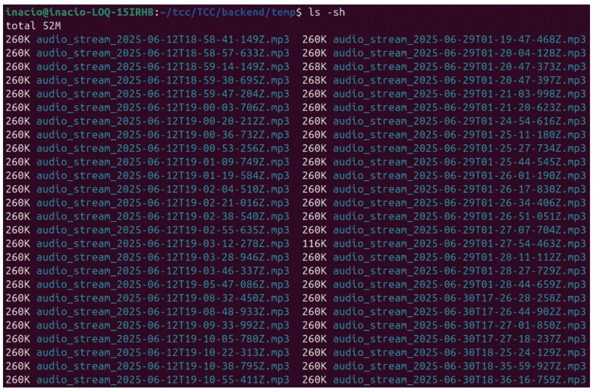

Figure 9: Digital audio payload files buffered and accumulated by the telemetry system. Source: Author.

5.2 Server Infrastructure and Telemetry Dashboard

We deployed a Node.js REST (*Representational State Transfer*)-style API (*Application Programming Interface*) to ingest the HTTP POST requests (Fig. 10). The server autonomously executed SMTP (*Simple Mail Transfer Protocol*) protocols to dispatch emergency email alerts to predefined contacts upon receiving an interrupt flag from the hardware thresholds, implementing a scalable alert ingestion pipeline similar to those found in modern IoT frameworks (GHOSH et al., 2021).

We utilized MongoDB to index the telemetry data (Fig. 11), mapping physical device MAC (*Media Access Control*) addresses to corresponding user profiles, GPS coordinate histories, and 17 s MP3 audio blobs. This indexing strategy ensures rapid data retrieval and persistent storage for judicial review, consistent with data logging practices for high-reliability systems (PENCHALAIAH et al., 2021).

The React-based dashboard (Fig. 12) plotted incoming GPS coordinates on a Cartesian map interface, providing real-time visual confirmation of the hardware's location-tracking capabilities. Such visual telemetry interfaces are essential for enabling immediate response from emergency contacts or law enforcement (PATEL; HASAN, 2018).

Table 2: Empirical hardware performance metrics extracted during continuous validation polling.

Metric	Value	Condition
GPS Time-to-First-Fix (TTFF)	$\sim$35 s	Open sky environment
GPS positional accuracy	$\pm$3–5 m	Urban outdoor environment
Event-to-Server Latency	$<$2.0 s	Wi-Fi hotspot overhead
I2S Audio packet interval	1.0 s	Continuous capture
Audio file generation	17.0 s	Back-end MP3 conversion
Maximum current draw	360 mA	Active Wi-Fi + All sensors
Estimated minimum autonomy	$\sim$10 h	Continuous maximum stress

5.3 Empirical Performance Metrics

Table 2 consolidates the measured hardware parameters extracted during continuous validation polling. These values define the operational boundaries of the current ESP32-based configuration under active multi-sensor load, providing empirical baseline metrics for future optimizations based on SMD (*Surface-Mount Device*) components (HYNDAVI; NIKHITA; RAKESH, 2020; HWLibre, 2024).

The parameters in Table 2 establish the hard operational limits of this proof-of-concept iteration. The $\sim$35 s TTFF and $\pm$3–5 m positional error are consistent with u-blox NEO-7M module specifications under typical acquisition conditions. The $<$2.0 s event-to-server latency is the aggregated overhead of the Wi-Fi association, TCP (*Transmission Control Protocol*) handshake, and HTTPS payload delivery over a smartphone hotspot relay — a figure that is conditionally acceptable for a proof-of-concept but structurally inadequate for a real-time emergency system, where sub-second determinism is mandatory. The 360 mA continuous draw and $\sim$10 h stress autonomy together confirm that the current hardware bill of materials, centered on through-hole components and a general-purpose development board, does not satisfy the power budget of a deployable wearable device.

5.4 Hardware Prototype and Stress Profiling

We assembled the components onto the custom 73 $\times$ 92 mm PCB (Fig. 13) and enclosed the hardware within a 3D-printed chassis (Fig. 14). The resulting physical footprint is substantially larger than acceptable wearable tolerances, reinforcing the proof-of-concept nature of this iteration as discussed in hardware miniaturization literature (PENCHALAIAH et al., 2021).

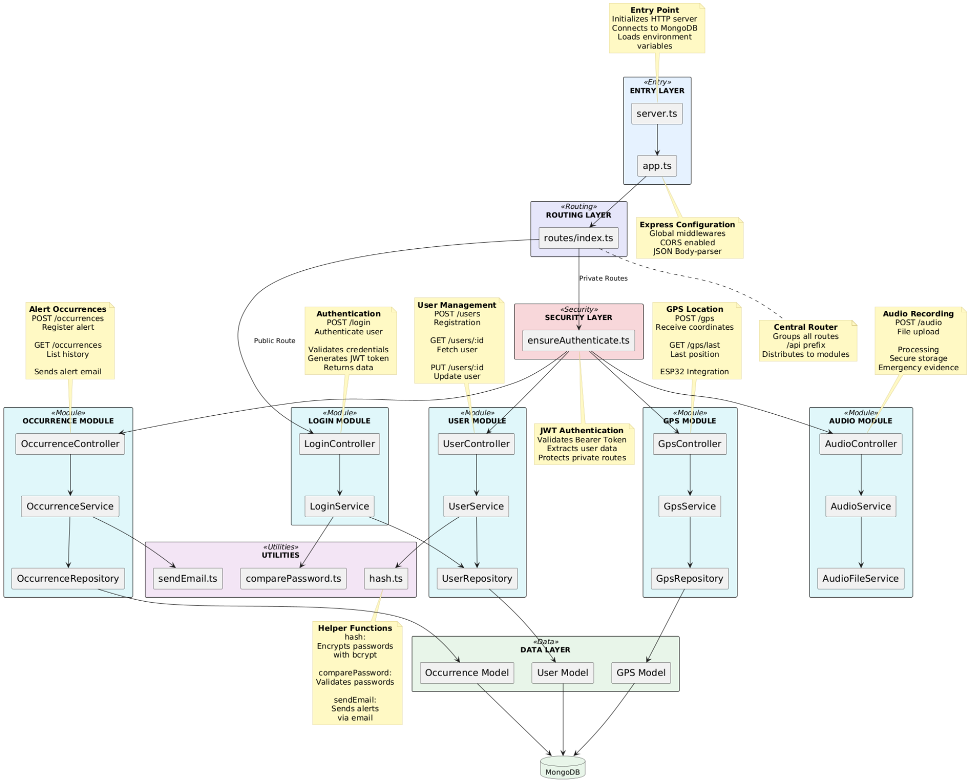

Figure 10: Architectural diagram of the Node.js server ingestion pipeline. Source: Author.

5.4.1 Power Profile and Continuous Drain

The system draws power from two series-connected 18650 lithium-ion cells, delivering 7.4 V with a theoretical 3600 mAh capacity. To validate the hardware limits, we executed a continuous stress protocol, forcing the ESP32 to simultaneously poll the GPS, read the IMU (*Inertial Measurement Unit*) vectors, stream I2S audio, and hold an active Wi-Fi transmission socket, testing the endurance limits of the current power management architecture (SYSTEMS, 2024; GHOSH et al., 2021).

5.4.2 Empirical Stress Test Results

We measured the current draw via an ammeter inserted in series with the battery load. Under the continuous transmission stress protocol, the system sustained a maximum current draw of 360 mA. Applying the 3600 mAh capacity, this results in a theoretical maximum continuous runtime of approximately 10 hours. This is under maximum load scenarios, with all sensors and actuators activated, which is not feasible for everyday use.

6 Discussion

Existing commercial devices often depend heavily on active user triggering, rendering them ineffective during sudden attacks (PATEL; HASAN, 2018). The results obtained in this work demonstrate the technical feasibility of integrating multiple geolocation, motion, and audio sensors in a system based on the ESP32 microcontroller for monitoring and alerting in risk situations faced by women. The prototype establishes a baseline for deterministic, automated distress signaling without requiring active user intervention. These findings corroborate the architectural approaches proposed by Hyndavi *et al.* (HYNDAVI; NIKHITA; RAKESH, 2020) and Penchalaiah *et al.* (PENCHALAIAH et al., 2021), confirming that the ESP32 possesses sufficient bandwidth for simultaneous UART, I2C, and I2S bus polling. The developed proof of concept confirms that the proposed architecture, comprising data collec-

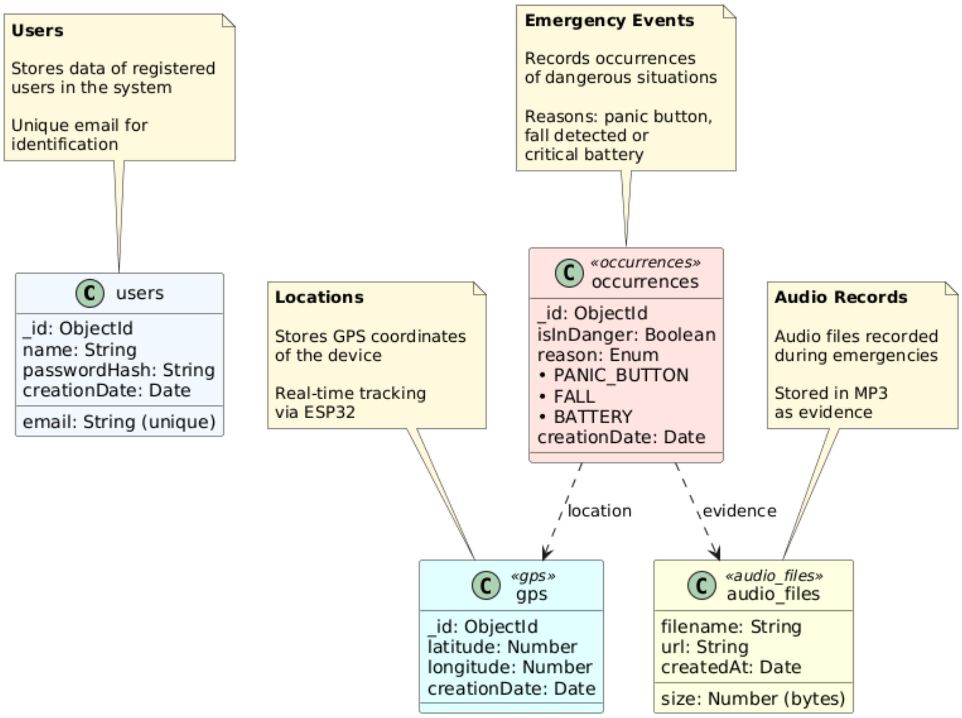

Figure 11: MongoDB schema structure for telemetry archiving. Source: Author.

tion via sensors, processing in a Node.js *back-end*, storage in MongoDB, and visualization through a React interface, is functionally adequate for personal security applications. This approach is aligned with the broader trend toward intelligent monitoring systems, in which deep learning is increasingly applied to wearable data for automatic activity and risk detection (ZHANG et al., 2022).

In the context of violence against women, the microphone plays a relevant role by enabling the capture of sounds and voices, even in restricted environments. In addition to enabling the immediate triggering of alerts when the victim cannot manually activate the device, audio recording can serve as concrete evidence in judicial proceedings, supporting investigations and increasing the chances of holding the aggressor accountable (MURALEEDHARAN; GARCIA-CONSTANTINO, 2022). Muraleedharan and Garcia-Constantino (2022) (MURALEEDHARAN; GARCIA-CONSTANTINO, 2022) demonstrated that audio-based systems can identify sound patterns characteristic of assaults, highlighting a promising and still little-explored approach to improve intelligent personal security architectures. Also, the choice of the ESP32 microcontroller proved adequate due to its integrated *Wi-Fi* connectivity, *dual-core* processing, and availability of I2C and I2S interfaces. Compared to Raspberry Pi-based solutions, the ESP32 offers significantly lower energy consumption, which is fundamental for continuous operation.

Unlike the other works mentioned above, this project makes the firmware repository publicly available, which represents an important contribution of this research. Thus, we have established a reproducible basis for the integration of sensors and embedded processing, while also allowing future studies to focus on overcoming the challenges of miniaturization and energy efficiency.

6.1 Limitations

It is acknowledged that the developed artifact constitutes a proof of concept of a wearable device, rather than a final commercial wearable product. This limitation stems primarily from constraints in laboratory infrastructure and availability of specialized electronic components. The development of truly wearable devices re-

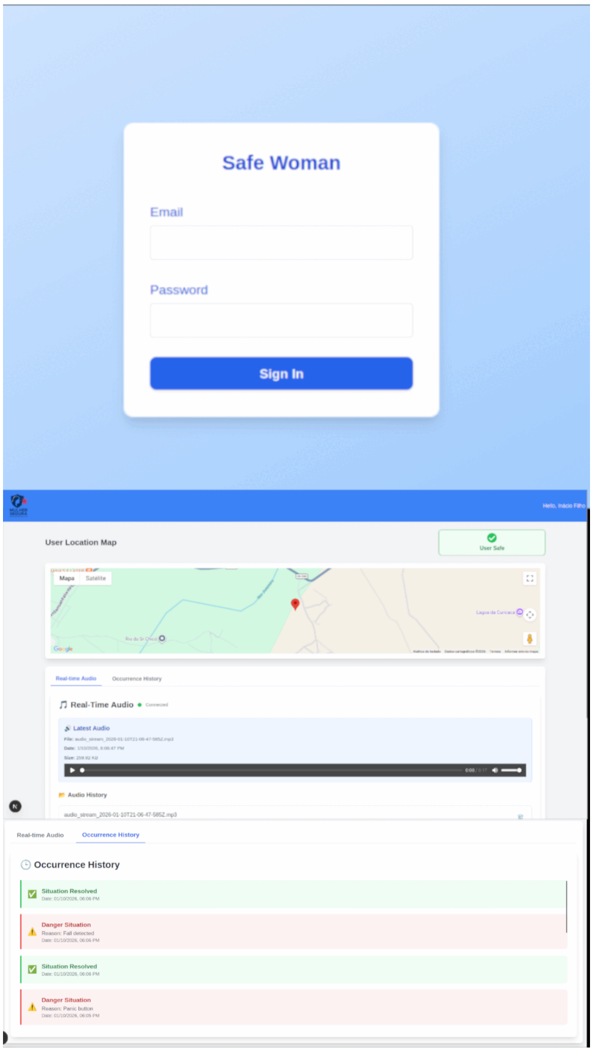

Figure 12: Telemetry dashboard executing real-time coordinate mapping and flag alerts. Source: Author.

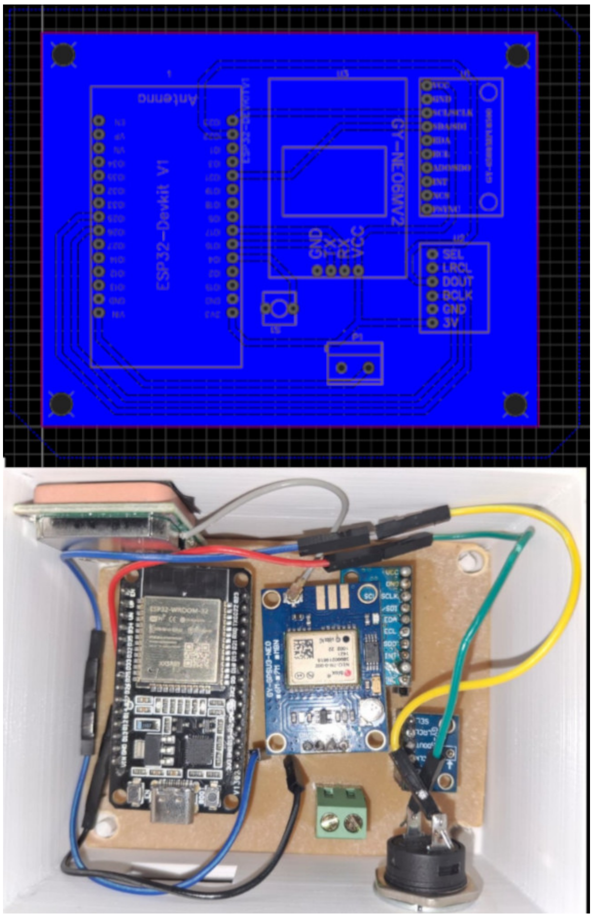

Figure 13: Milled 73 $\times$ 92 mm PCB and populated hardware components. Source: Author.

Figure 14: Fully assembled hardware prototype within the 3D-printed enclosure. Source: Author.

quires SMD technology components, multilayer printed circuit boards with reduced dimensions, and specialized equipment for miniaturized assembly. The 73×92 mm PCB footprint, fabricated using standard components, renders the device too bulky for practical, discreet integration into everyday clothing. While we designed the current enclosure for belt mounting, true wearable autonomy requires drastic miniaturization. Viswanath *et al.* (VISWANATH; PAKYALA; MUNEESWARI, 2016) and Ghosh *et al.* (GHOSH et al., 2021) present similar limitations in their prototypes, highlighting the gap between the nomenclature used and the actual technological maturity of academic devices.

The architecture's dependency on a victim-owned smartphone to sustain the Wi-Fi hotspot constitutes a structural design failure that goes beyond simple engineering inconvenience. Studies on domestic violence and intimate partner aggression consistently document that aggressors confiscate, physically destroy, or remotely isolate the victim's mobile phone as a primary control mechanism during assault events (KOUZANI, 2023). Future hardware revisions must therefore unconditionally eliminate the smartphone dependency by integrating a dedicated cellular IoT modem — specifically a SIM7000-series module supporting LTE-M (*Long-Term Evolution for Machines*) Cat-M1 and NB-IoT (*Narrowband IoT*) — directly onto the wearable PCB.

The hardware analysis also identified challenges related to the power budget. The continuous active current draw of approximately 360 mA may limit the operational autonomy expected for wearable devices. Although the use of the ESP32 provides considerable power savings compared to microprocessor-based solutions such as the Raspberry Pi adopted by Ghosh *et al.* (GHOSH et al., 2021), the current architecture still results in relatively high energy consumption, reducing the runtime of the 7.4 V battery configuration under intensive operation.

7 Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

8 Conclusion

This study engineered and tested a proof of concept of a wearable device designed to automate physical distress signaling. The empirical validation confirmed that an ESP32 microcontroller possesses the hardware bandwidth to concurrently sample I2C kinematic vectors, UART GPS coordinates, and I2S digital audio, executing real-time threshold evaluations to trigger alerts without manual intervention. The associated Node.js and React telemetry infrastructure successfully archived and mapped the resulting data payloads.

Future engineering iterations must improve the current hardware layout. Subsequent development requires a transition to miniaturized SMD architectures utilizing low-power PMICs (*Power Management Integrated Circuits*) and high-density LiPo (*Lithium Polymer*) cells. To eliminate the smartphone dependency, the microcontroller must integrate a dedicated LTE-M or NB-IoT baseband modem, operating under aggressive deep-sleep schedules interrupted exclusively by IMU-driven hardware wakes.

Additionally, the development of commercial-grade wearable prototypes within academic research laboratories remains a significant challenge due to limited access to specialized manufacturing equipment, compact fabrication technologies, and industrial-grade materials. These constraints directly impact device miniaturization, energy optimization, enclosure quality, and long-term reliability, often restricting academic prototypes to proof-of-concept implementations rather than fully deployable consumer products.

References

BHUVANESWARI, V. S. S. S.; THANGAMUTHU, M. Towards intelligent safety: A systematic review on assault detection and technologies. **Sensors**, MDPI, v. 25, n. 13, p. 3985, 2025.

DIAN, F. J.; VAHIDNIA, R.; RAHMATI, A. Wearables and the internet of things (iot), applications, opportunities, and challenges: A survey. **IEEE Access**, IEEE, v. 8, p. 69200–69211, 2020.

FAROOQ, M. S.; MASOOMA, A.; OMER, U.; TEHSEEN, R.; GILANI, S.; ATAL, Z. The role of iot in woman's safety: A systematic literature review. **IEEE Access**, IEEE, v. 11, p. 69807–69825, 2023.

GARCÍA-MORENO, C.; PALLITTO, C.; DEVRIES, K.; STÖCKL, H.; WATTS, C.; ABRAHAMS, N. **Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence**. Geneva: World Health Organization, 2013.

GHOSH, P.; BHUIYAN, T. M.; NIBIR, M. A.; HASAN, M. E.; ISLAM, M. R.; HASAN, M. R.; HOSSAIN, T. Smart security device for women based on iot using raspberry pi. In: IEEE. **2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)**. Dhaka, Bangladesh, 2021. p. 57–60.

HWLibre. **How to use the SPH0645LM4H microphone with Arduino and Raspberry Pi**. 2024. Disponível em: <https://en.hwlibre.com/How-to-use-the-sph0645lm4h-microphone-with-arduino-and-raspberry-pi/>.

HYNDAVI, V.; NIKHITA, N. S.; RAKESH, S. Smart wearable device for women safety using iot. In: IEEE. **2020 5th International Conference on Communication and Electronics Systems (ICCES)**. Coimbatore, India, 2020. p. 459–463.

ISLAM, N.; HOSSAIN, M. R.; ANISUZZAMAN, M.; OBAIDULLAH, A. J. M.; ISLAM, S. S. Design and implementation of women auspice system by utilizing gps and gsm. In: IEEE. **2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)**. Cox's Bazar, Bangladesh, 2019. p. 1–6.

KASHALKAR, K. **Getting started with ublox Neo 7M GPS module for Arduino**. 2021. Blog post. Disponível em: <https://koustubhkashalkar.wordpress.com/2021/08/13/getting-started-with-ublox-neo-7m-gps-module-for-arduino/>.

KOUZANI, A. Z. Technological innovations for tackling domestic violence. **IEEE Access**, IEEE, v. 11, p. 91293–91311, 2023.

MURALEEDHARAN, A.; GARCIA-CONSTANTINO, M. Domestic violence detection using smart microphones. In: SPRINGER. **International Conference on Ubiquitous Computing and Ambient Intelligence**. Cham, 2022. p. 357–368.

PATEL, J.; HASAN, R. Smart bracelets: Towards automating personal safety using wearable smart jewelry. In: IEEE. **2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)**. Las Vegas, NV, USA, 2018. p. 1–2.

PENCHALAIAH, N.; SUSMITHA, M.; REDDY, C. V. K.; RAO, D. P. K.; SREELEKHA, D. An iot based smart wearable device for women safety. **International Research Journal on Advanced Science Hub**, v. 3, n. 5S, p. 89–95, 2021.

SYSTEMS, E. **ESP32 Series Datasheet**. Shanghai, 2024. Disponível em: <https://docs.espressif.com/projects/esp-dev-kits/en/latest/esp32/esp32-devkitc/user_guide.html>.

VISWANATH, N.; PAKYALA, N. V.; MUNEESWARI, G. Smart foot device for women safety. In: IEEE. **2016 IEEE region 10 symposium (TENSYMP)**. [S.l.], 2016. p. 130–134.

WAGH, N. R.; SUTAR, S. R.; KADAM, V. J.; JADHAV, S. M.; YADAV, A. S.; PAWAR, V. S. Evaluation of iot based smart safety systems for women and children using machine learning techniques. **Scientific Reports**, Nature Publishing Group, v. 15, 2025.

ZHANG, S.; LI, Y.; ZHANG, S.; SHAHABI, F.; XIA, S.; DENG, Y.; ALSHURAFA, N. Deep learning in human activity recognition with wearable sensors: A review on advances. **Sensors**, MDPI, v. 22, n. 4, p. 1476, 2022.

ZIKRIYA, M.; PARMESHWAR, M.; MATH, S. R.; TANKASALI, S.; MALLAPUR, J. D. Smart gadget for women safety using iot (internet of things). **International Journal of Engineering Research & Technology (IJERT)**, v. 6, n. 13, 2018.