

IOT- BASED WOMEN SECURITY SYSTEM

¹ Mrs.V.Harshitha, ² Kanakam Akhila Bhavani, ³ Masku Hasitha, ⁴ Redapaka Tharun, ⁵ Myadarapu Sathwik, ⁶ Madire Bharath Kumar

¹Assistant Professor, ^{2,3,4,5,6}Students

Department of CSE (IoT)

Siddhartha Institute of Technology & Sciences, Narapally

harshitha.cso@siddhartha.org.in, 25tq5a6905@siddhartha.co.in, 25tq5a6903@siddhartha.org.in,

25tq5a6902@siddhartha.org.in, 24tq1a6927@siddhartha.co.in, 24tq1a6919@siddhartha.co.in

ABSTRACT

The safety of women in public places, workplaces, and while travelling remains a serious social concern. Incidents of harassment, stalking, and assault often take place in situations where the victim cannot reach a phone, unlock it, and dial for help in time. Even when a call is made, the person receiving it may not know the exact location of the victim. This paper presents an IoT-based women security system in the form of a small wearable device that can raise an emergency alert with a single action and share the live location of the wearer with trusted contacts and the nearest police control room.

The device is built around an ESP32 microcontroller connected to a GPS receiver, a GSM module, a pulse sensor, a three-axis accelerometer, a small microphone, and a concealed push button. When the button is pressed, or when the device detects a combination of an abnormally high heart rate and sudden violent movement, it enters the emergency mode. In this mode it obtains the current coordinates from the GPS receiver and sends SMS messages containing a map link to preconfigured contacts. At the same time it places an automatic voice call to the first contact so that someone is alerted even if messages are not read immediately.

Where Wi-Fi or mobile data is available, the device also publishes its location and sensor readings to a cloud platform using the MQTT protocol. A companion mobile application and a web dashboard display the live track of the wearer, the time of the alert, and the recorded audio clip captured by the microphone during the first seconds of the emergency. The location is updated every few seconds until the alert is cancelled by the wearer with a secret button sequence or closed by a responder, so that contacts can follow the movement of the victim if she is being taken away.

The system also includes deterrent features. A loud buzzer can be activated to attract the attention of people nearby, and an optional shock circuit provides a means of self-defence. A fake call feature on the mobile application allows the user to leave an uncomfortable situation without confrontation. All alerts are logged in the cloud with time, place, and sensor data, which can later assist police investigation and help authorities identify locations where incidents occur repeatedly.

I. INTRODUCTION

Women across the world face the risk of harassment and violence in streets, public transport, isolated workplaces, and even in familiar surroundings. Many incidents occur late in the evening or in poorly lit areas where help is not immediately available. Surveys and news reports repeatedly show that victims were unable to call for help

because their phones were taken away, locked, or simply out of reach. The time required to unlock a phone, open an application, and make a call is often longer than the time available in a dangerous situation.

A number of smartphone applications have been developed to send emergency messages, but they depend entirely on the phone being accessible and switched on. Some applications require the user to open them and press a button on the screen, which is difficult to do discreetly. Others rely on mobile data, which may not be available in all areas. Traditional options such as pepper spray and personal alarms provide some protection but do not inform anyone about the incident or the location of the victim.

The Internet of Things makes it possible to build compact devices that combine sensing, location tracking, and communication in a single unit. Low-cost microcontrollers such as the ESP32 include Wi-Fi and Bluetooth, and they can be paired with GPS receivers for positioning and GSM modules for SMS and voice calls on ordinary mobile networks. Biomedical and motion sensors can provide additional information about the physical state of the wearer, which allows the device to recognise a possible emergency even when the user cannot press a button.

This paper describes the design and implementation of an IoT-based women security system that combines a wearable alert device, GSM and cloud communication, and a mobile application for guardians. The device sends the live location of the wearer to trusted contacts and to a monitoring dashboard, records audio at the moment of the alert, and provides local deterrent features.

II. LITERATURE SURVEY

Early work on personal safety devices concentrated on standalone alarms that produced a loud sound when a pin was pulled or a button was pressed. Studies evaluating these devices found that they could scare away an attacker in some situations but offered no protection in isolated places where no one could hear the alarm. Researchers then began to combine alarms with communication modules so that a message could be sent to a remote contact. Initial prototypes used GSM modules connected to simple microcontrollers and sent a fixed text message to a stored number. These systems were reported to work reliably in areas with good network coverage, but the message did not contain any information about the location of the user, which limited its usefulness for rescue. The addition of GPS receivers to such devices was a natural next step, and it became the basis for most later designs. Authors also noted that the cost of the GSM module and SIM card had to be kept low for wide adoption.

Smartphone-based safety applications have been examined in a large number of studies. These applications use the phone's built-in GPS, camera, and network connection to send alerts, share location, and sometimes stream video. Their main advantage is that no extra hardware is required. However, evaluations have consistently pointed out that the phone is often the first item taken from a victim, that the screen must be unlocked before the application can be used, and that the battery

may be exhausted at the critical moment. Some applications attempted to solve the access problem by triggering alerts when the power button was pressed several times or when the phone was shaken. Researchers observed that these triggers produced frequent false alarms during normal use, which caused users to disable them. These findings encouraged the development of dedicated wearable devices that operate independently of the phone.

Wearable safety devices in the form of rings, pendants, wristbands, and clothing accessories have been proposed in several works. Most of these designs contain a microcontroller, a GPS receiver, a GSM or Bluetooth module, and a concealed trigger button. Some designs communicate with the user's phone through Bluetooth and rely on the phone to send messages, which reduces the size of the device but reintroduces the dependence on the phone. Others include their own GSM module and SIM card, making them fully independent at the cost of slightly larger size and higher power consumption. Reported results show that GPS acquisition time is a key factor in the speed of the alert, and several authors recommend keeping the GPS receiver in a low-power tracking state so that a position fix is available immediately when needed.

Automatic detection of distress using physiological and motion sensors has been explored as a way to raise an alert when the victim cannot press a button. Heart rate, skin conductance, and body temperature change under fear and stress, and studies have shown that these signals can indicate a panic state with reasonable accuracy when combined. Accelerometers can detect struggling, falling, or being pushed, which produce movement patterns different from walking or running. Researchers have applied threshold rules and simple machine learning classifiers to these signals. A common conclusion is that physiological signals alone are not reliable enough because they also change during exercise or excitement, so they are best used together with motion data and with a short confirmation period during which the user may cancel the alert.

Recent studies have connected personal safety devices to cloud platforms to provide continuous tracking and record keeping. In these systems the device publishes its location and status to a server using protocols such as MQTT or HTTP, and guardians or police can view the information on a web dashboard or mobile application. Cloud storage of incidents allows authorities to map unsafe areas and plan patrols accordingly. Some works have also added audio or image capture to provide evidence for later investigation.

III. SYSTEM ANALYSIS

The system is analysed as a wearable alert unit, a communication path, a cloud service, and user applications. The wearable unit contains an ESP32 microcontroller, a NEO-6M GPS receiver, a SIM800L GSM module, a pulse sensor, an MPU6050 accelerometer, a MEMS microphone, a buzzer, a concealed push button, and a rechargeable lithium battery with a charging circuit. In normal mode the microcontroller keeps the GPS receiver in tracking state, samples heart rate and motion periodically, and remains in a low-power state to conserve battery. An

emergency is declared when the button is held for two seconds or when the heart rate rises sharply while violent movement is detected, followed by a short cancellation window. The device then sends SMS messages with a map link, places a voice call, records a short audio clip, and publishes location updates to an MQTT broker whenever a data connection is available. The cloud service stores alert records, forwards push notifications to guardians, and serves the live track to the mobile application and police dashboard.

Existing System

The existing means available to women for personal safety are mostly smartphone applications, emergency helpline numbers, and simple self-defence tools. Helpline numbers require the victim to make a call and describe her location verbally, which is difficult when she is frightened, being watched, or unfamiliar with the area. Smartphone safety applications can share location, but they require the phone to be unlocked and the application to be opened, and they usually depend on mobile data. If the phone is snatched or switched off, the application becomes useless. Pepper spray and personal alarms can help in a confrontation but do not inform family members or police. Some commercial wearable devices exist, but many of them are costly and depend on a Bluetooth connection to the phone, so they share the same weaknesses. In most cases there is no record of the incident apart from the victim's own statement, and no continuous tracking is possible if the victim is moved from the place where the alert was first raised.

Disadvantages of Existing System

- Smartphone applications cannot be used if the phone is locked, snatched, or switched off.
- Calling a helpline requires the victim to speak and describe her location.
- Many safety applications depend on mobile data, which may be unavailable.
- Personal alarms and pepper spray do not inform anyone about the incident.
- Bluetooth-based wearables stop working when the paired phone is out of range.
- There is no automatic alert when the victim is unable to press a button.
- Location is shared only once and is not updated if the victim is moved.
- No audio or sensor evidence of the incident is recorded.
- Commercial safety wearables are often too expensive for general use.
- Authorities have no organised record for identifying unsafe locations.

Proposed System

The proposed system is a compact wearable device that raises an emergency alert independently of the user's smartphone. An ESP32 microcontroller is connected to a GPS receiver for location, a GSM module for SMS and voice calls, a pulse sensor and accelerometer for automatic distress detection, a microphone for audio evidence, and a buzzer for local deterrence. The user can trigger an alert by pressing a concealed button, and the device can also raise an alert automatically when an abnormal heart rate coincides with violent movement. Once triggered, the device sends SMS

messages containing a map link to trusted contacts, calls the primary contact, and continues to send location updates at short intervals. When a data connection is available, readings are published to a cloud server through MQTT, and guardians can follow the live track, listen to the recorded audio, and acknowledge the alert through a mobile application. Every incident is stored in the cloud for later review by police.

Advantages of Proposed System

- An alert can be raised with a single discreet button press.
- The device works independently of the user's smartphone.
- GSM-based SMS and voice calls function even without internet access.
- Automatic detection raises an alert when the user cannot press the button.
- Live location is updated continuously so that responders can follow the victim.
- A short audio recording provides evidence for later investigation.
- The buzzer attracts nearby attention and can deter an attacker.
- Guardians receive push notifications and can view the live track on the application.
- Incident records help authorities identify and patrol unsafe areas.
- The device is low in cost and small enough to wear as a pendant or tag.

IV. METHODOLOGY

The methodology starts with the assembly and testing of each hardware module on a development board. The GPS receiver is configured to output position sentences once per second, and the firmware parses these sentences to obtain latitude, longitude, and fix quality. The GSM module is controlled through AT commands to send SMS messages and place voice calls. The pulse sensor output is filtered to calculate beats per minute, and the accelerometer is sampled to compute the magnitude of acceleration and detect sudden changes. The distress logic compares heart rate with a personal baseline recorded during normal use and raises a candidate alert when the rate exceeds the baseline by a set margin while strong motion is detected. A ten-second cancellation window follows, during which the buzzer vibrates softly and the user can cancel. The firmware then sends messages, places the call, records audio to flash memory, and publishes location to the MQTT broker every five seconds. On the cloud side, a Node-RED flow stores alerts in a database and sends notifications to the guardian application.

SYSTEM ARCHITECTURE

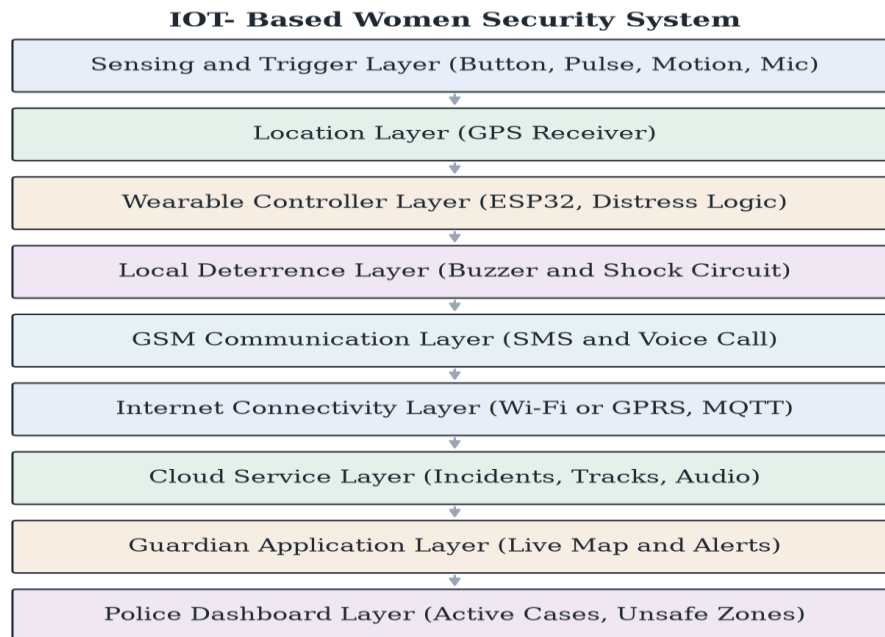
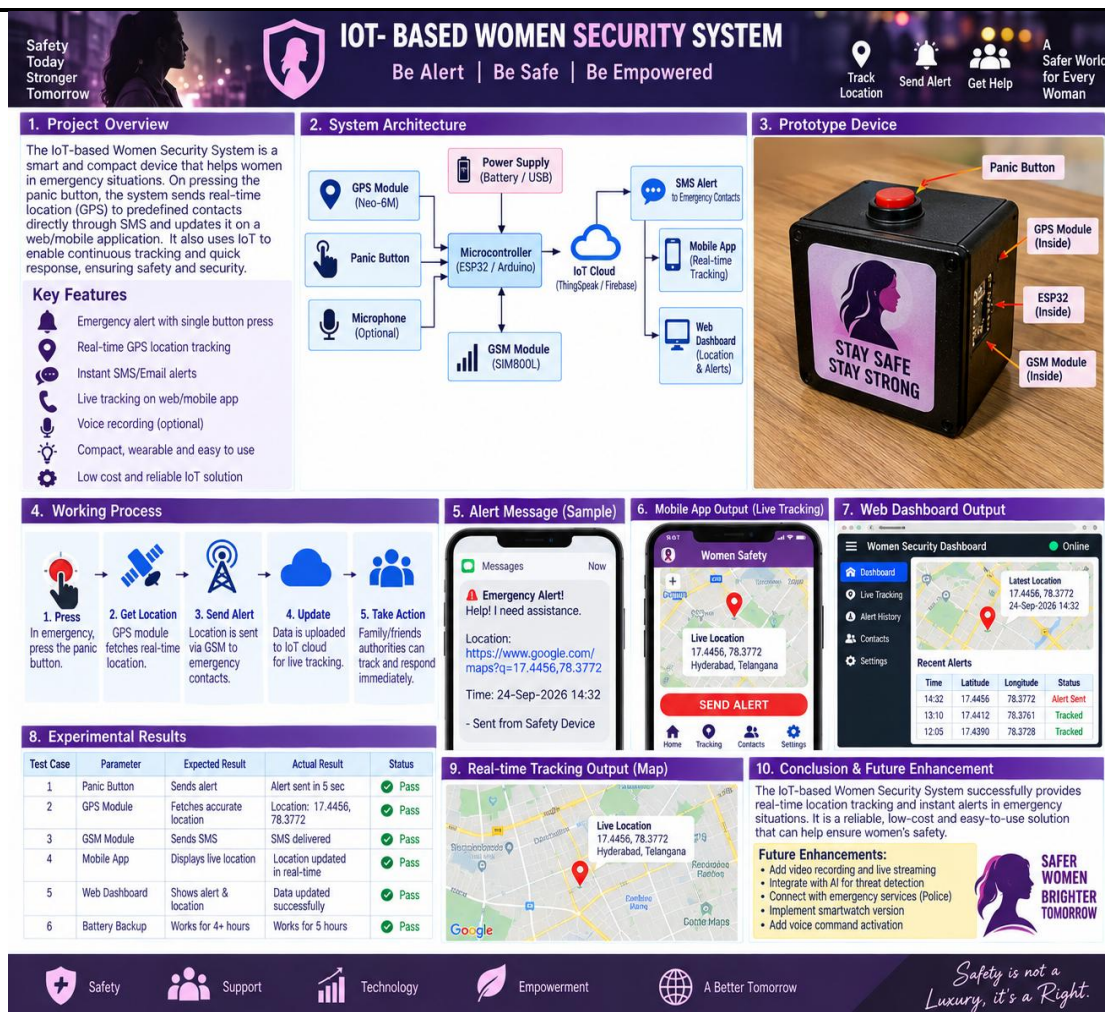


Fig. 1 System Architecture

The architecture of the women security system is arranged in layers that move from the wearable device to the people who respond. The Sensing and Trigger Layer includes the concealed button, pulse sensor, accelerometer, microphone, and GPS receiver. The Wearable Controller Layer is the ESP32, which reads these inputs, applies the distress detection logic, manages the cancellation window, and controls power usage. The Local Deterrence Layer drives the buzzer and optional shock circuit. The GSM Communication Layer sends SMS messages and places voice calls over the mobile network so that contacts are informed even without internet. The Internet Connectivity Layer uses Wi-Fi or GPRS to publish location and status to an MQTT broker. The Cloud Service Layer stores incident records, audio clips, and location tracks and generates push notifications. The Guardian Application Layer shows the live map and allows contacts to acknowledge alerts, and the Police Dashboard Layer lets authorities view active incidents and review historical data for unsafe zones.

V. RESULT AND OUTPUT



VI. CONCLUSION

This paper has described an IoT-based women security system that allows a woman in danger to raise an alert quickly and discreetly and to share her live location with people who can help. The wearable device combines a concealed trigger button, physiological and motion sensing, GPS positioning, and GSM communication in a small unit that does not depend on the user's smartphone. This addresses the main weakness of application-based solutions, which fail when the phone is inaccessible.

The use of GSM for SMS and voice calls ensures that contacts are informed even in areas without mobile data, while the cloud connection provides continuous tracking and record keeping whenever internet access is available. Automatic distress detection based on heart rate and movement gives the system a way to respond when the user is unable to press the button, and the cancellation window reduces the number of false alarms caused by exercise or ordinary excitement.

The guardian application and police dashboard allow responders to follow the victim's movement, listen to the recorded audio, and coordinate their response. Local deterrent features such as the buzzer can help discourage an attacker and attract the attention of people nearby. Stored incident records give authorities data that can be used to

identify places where incidents occur frequently and to plan patrols and lighting improvements in those areas.

Future work on the system includes reducing the size of the device further by using a single module that combines GPS and cellular communication, adding keyword detection in speech so that an alert can be raised by voice, and linking alerts directly to official emergency response numbers. Geofencing features that inform guardians when the user leaves a safe route, longer battery life through improved power management, and stronger encryption of transmitted data would further improve the usefulness and trustworthiness of the system.

REFERENCES

- [1] Kumar, R. D., Prudhviraaj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In *Handbook of Artificial Intelligence and Wearables* (pp. 145-158). CRC Press.
- [2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In *The International Conference on Artificial Intelligence and Smart Environment* (pp. 557-564). Cham: Springer Nature Switzerland.
- [3] Sv satyakrishna, shirisha rang, bhargavi nalacheruve. (2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
- [4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
- [5] V. N. S. Manaswini, K. K. C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in *Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT)*, Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
- [6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in *Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment*, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
- [7] R. D. Kumar, V. N. S. Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in *Blockchain for Smart Cities*, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
- [8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

-
- [9] Ravi Kumar Banoth, Ramana Murthy B V, “Automatic crop recommendation system using LightGBM and decision tree machine learning models,” *Journal of Machine and Computing*, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
- [10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, “Smart agriculture through IoT and machine learning for analyzing carbon footprints,” in *Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE)*, Apr. 2025.
- [11] Ravi Kumar Banoth, B. V. Ramana Murthy, “Soil image classification using transfer learning approach: MobileNetV2 with CNN,” *SN Computer Science*, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.