JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IOT BASED SYSTEM FOR WOMEN SAFETY

[1]Parameswari P, [2]Balasubramaniam K R, [3]Hariharan K, [4]Akil K

[1]Assistant Professor, [234]UG Students
[1234] Department of Computer Science and Engineering
[1234]Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu, India

Abstract : The "IoT-Based System for Women Safety" project presents a clever solution to tackle the pressing issue of women's safety. By harnessing the power of the Internet of Things (IoT), this system offers real-time monitoring and assistance in potentially risky situations. It brings together a network of IoT devices, including small discreet wearables, mobile apps, and strategically positioned sensors in public areas, ensuring women's security through seamless connectivity. The wearable devices are equipped with GPS, panic buttons, and biometric sensors, enabling quick notifications to authorities and loved ones in emergencies. To empower users, a dedicated mobile app allows them to interact with the system, offering features like location tracking, access to emergency services, and a supportive community network. In public spaces, special sensors are deployed to promptly detect any suspicious activities and alert the relevant authorities. The data collected from these devices is processed and securely stored in the cloud, facilitating continuous monitoring and analysis using advanced machine learning algorithms. Moreover, this system actively encourages community involvement by allowing users to share safety concerns, receive real-time alerts from nearby individuals, and collaborate with local authorities and support networks. It establishes a dependable safety net by combining preventive and reactive measures, thereby bolstering women's security and fostering confidence, ultimately contributing to the creation of a safer society.

IndexTerms **- Internet of Things, Smart Women Safety, GSM/GPS module, sensors.**

I. INTRODUCTION

In recent years, women's safety has become a paramount global concern. Despite existing safety measures, a more versatile and proactive solution is necessary. Our project aims to bridge the gap by using IoT technology to create an efficient and user-centric safety system. The goal is to empower women with real-time monitoring, quick response mechanisms, and a supportive community network. Due to the high prevalence of violence against women and limitations of existing safety measures, an innovative approach is necessary. Traditional methods often rely on smartphones, which may not be accessible in emergencies. Our proposed system uses discreet wearables with GPS, panic buttons, and biometric sensors as an interface for users to initiate safety measures. The system includes sensors in public areas to detect suspicious activities, providing comprehensive safety measures. Data is securely stored in the cloud for continuous monitoring and analysis using advanced machine learning algorithms. Our project focuses on user empowerment through a mobile app with features like location tracking, emergency services, and a community network. By involving the community and utilizing local authorities and support networks, our system enhances women's safety. This paper reveals the IoT-based safety system's architecture and development methodology. The following sections will discuss the literature, our proposed system, methodology outcomes, and future enhancements.

II. LITERATURE REVIEW

Debojyoti Seth et.al [2018], IoT-based platforms enhance women's safety by seamlessly coordinating sensors and actuators. Hidden Markov Models enable dynamic predictive analysis, aiding dense detection of suspicious activities. Facial recognition and ambiguous conversation labeling contribute to situational analysis. In emergencies, the GSM/GPS module triggers alerts for aftershocks or notifies the wearer. Experimental results show promising accuracy at 94.7%. Keywords: IoT, HMM, Smart Woman Safety, GSM/GPS Module, Fuzzy. [1]

DhirajSunehra et.al [2020], Introducing a smart security solution using Raspberry Pi3 for women and children safety. This wearable device functions as an alarm and security system, alerting nearby individuals with a buzzer. Utilizing GPS and GSM/GPRS technology, it sends the user's location via SMS to emergency contacts and the police. A connected USB webcam captures images during an attack, and pressing the panic button triggers immediate email notifications with the images to emergency contacts. Keywords: Raspberry Pi3, IoT, GPS, GSM, email notification. [2]

Prottasha Ghosh et.al [2021], This paper introduces an innovative IoT-based safety device for women, comprising a compact system with a Raspberry Pi, flex sensor, buzzer, camera, GSM, and GPS modules. The device, discreetly embedded in women's underwear, activates upon hand movement, triggering an alarm, capturing images, and sending GPS location via SMS for immediate rescue. The Raspberry Pi and GSM modules enable communication, while a web server stores evidence, including images, videos, and audio, ensuring a reliable record for addressing safety concerns in vulnerable situations. [3]

Rahul Paknikar et.al [2019], Proposing a rural women's safety system using IoT, we suggest wearable devices with a distress button. When activated, the beacon sends emergency signals to a central station, triggering a village-wide alarm. GPS and Bluetooth Low Energy enable location tracking, overcoming rural connectivity challenges. The system utilizes solar panels for sustainability and ensures safety in areas with unreliable mobile networks. [4]

N.L. VamsiPriya.K et.al [2018], This project introduces a safety initiative for women, featuring a wearable device with an emergency button. When pressed, the device activates GPS, sending the victim's location and timestamp via SMS to pre-configured contacts, including the police. Worn as a watch or bracelet, this rapid response system aims to provide quick assistance in case of harassment, ensuring timely intervention and improved personal security. [5]

III. PROPOSED SYSTEM

Our security framework relies on wearable devices with GPS, push button, and biometric sensors (Figure 3.1). These wearables act as an interface, enabling users to initiate security measures promptly. The collaborative approach enhances security by connecting wearable devices and sensors in open areas. They communicate through an IoT platform, exchanging information to a cloud-based system for processing and storage. The cloud foundation uses a dedicated server to collect real-time client data for quick response and coordination. Integration with external services, especially IFTTT webhooks, improves the alarm feature, ensuring efficient and automatic assistance in critical situations. A mobile app complements wearables, providing users with an easy-to-use interface. It offers real-time location tracking, access to emergency services, and community engagement features, promoting safety and collaboration. Figure 6: Framework Design Piece Graph showcases the interconnected components of our security framework. The wearables, sensors, IoT platform, cloud infrastructure, and mobile app work together to create a comprehensive and responsive security network. [Square Graph Picture] The combined effort of these components ensures a rapid and effective response to dangers or crises, providing clients with enhanced security.

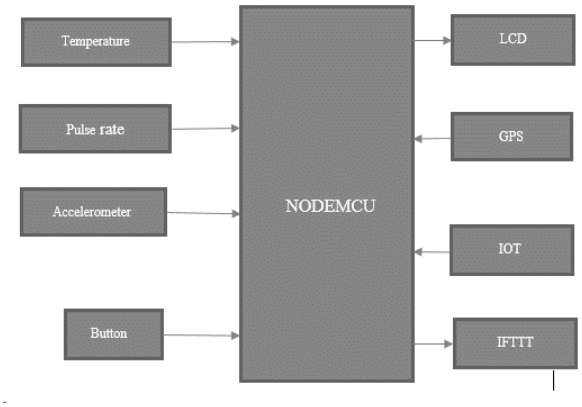

Fig 3.1: Proposed block diagram

IV. SYSTEM ARCHITECTURE

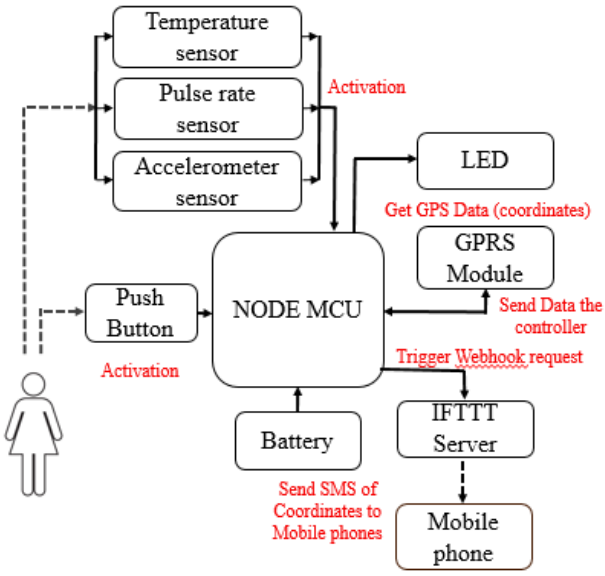

Fig 4.1: System Architecture of proposed

Figure 4.1 outlines the complicatedly planned design of a cutting-edge security framework that coordinating wearable gadgets, progressed sensors, cloud-based foundation, and machine learning calculations. At its center are wearable gadgets prepared with GPS modules, pulse-rate sensors, temperature sensors, and freeze buttons, serving as the essential client interface for collaboration with the security framework. The GPS module guarantees exact area following, whereas wellbeing parameters are ceaselessly observed through pulse-rate and temperature sensors, contributing to proactive risk location.

Encouraging consistent communication between wearable gadgets and the central server is the Web of Things (IoT) stage. This communication, frequently executed through conventions like MQTT or HTTP, empowers low-latency and proficient information exchange, guaranteeing real-time overhauls and quick reaction capabilities. The information collected from wearables is at that point transmitted to a cloud-based foundation, facilitated on stages such as Amazon Web Administrations or Microsoft Sky blue. This cloud framework serves as a secure store for client information, permitting for adaptable capacity, recovery, and investigation, improving the system's versatility.

Inside the cloud framework, a devoted server forms approaching information and stores it in a secure database. This server plays a significant part in executing complex calculations related to danger discovery, client profiling, and communication conventions. The database, whether social or NoSQL, stores verifiable and real-time information, supporting persistent observing and investigation of client data. To assist improve the system's capabilities, machine learning calculations are utilized for real-time investigation of client information. These calculations contribute to the mechanized mechanism's capacity to identify inconsistencies in wellbeing parameters and development designs, with the demonstrate advancing over time to make strides exactness. The design too joins a committed portable application, working as a client interface and control center. This application empowers clients to connected with the framework, track their security parameters, and physically actuate security instruments. Furthermore, the versatile app gives real-time cautions, area following, and community highlights, cultivating a collaborative approach to security. The outside administrations integration, especially with On the off chance that This At that point That (IFTTT) webhooks, fortifies the caution instrument. IFTTT webhooks encourage consistent communication between the framework and predefined contacts or crisis administrations, guaranteeing incite caution alacrity and facilitated reactions for effective help.

V. METHODOLOGY

The strategy connected within the advancement includes two unmistakable approaches:

A manual component and an robotized component. Within the manual strategy, clients take an dynamic part by starting security measures through a button press on the wearable gadget, as delineated in Figure 5.1. The NodeMCU expeditiously reacts to this enactment, activating a facilitated reaction. Utilizing the GPS module, the framework quickly obtains exact arranges, encouraging

exact area following. At the same time, an caution is produced, informing predefined crisis contacts. This hands-on instrument engages clients to flag trouble straightforwardly, pivotal in scenarios requesting prompt activity.

On the other hand, the mechanized component coordinating nonstop wellbeing checking and danger location. Leveraging advanced sensors inside the wearable gadget, the pulse-rate sensor acts as a steady gatekeeper, checking the user's heart rate. The DHT11 temperature sensor serves as a watcher, giving real-time temperature readings. The ADXL345 accelerometer sensor acts as a movement locator, measuring speeding up to distinguish bizarre developments or falls. The amalgamation of these sensors upgrades the system's capacity to distinguish potential dangers or crises without coordinate client intercession.

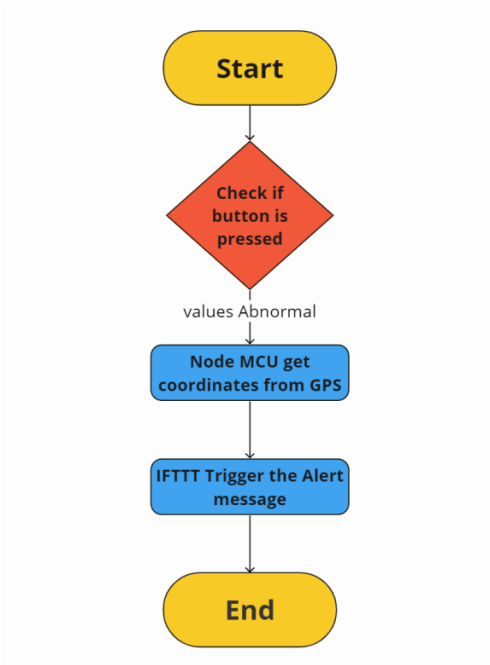

Fig 5.1: Flowchart for Manual Mechanism

The control stream of the robotized component is delineated in Figure 5.2, illustrating the precise prepare through which the framework analyzes sensor information and starts reactions. The pulse-rate sensor, temperature sensor, and accelerometer sensor collectively contribute to a security net past manual mediation. This layered approach guarantees upgraded unwavering quality, with the combined control of these three sensors giving a comprehensive and precise evaluation of the user's well-being.

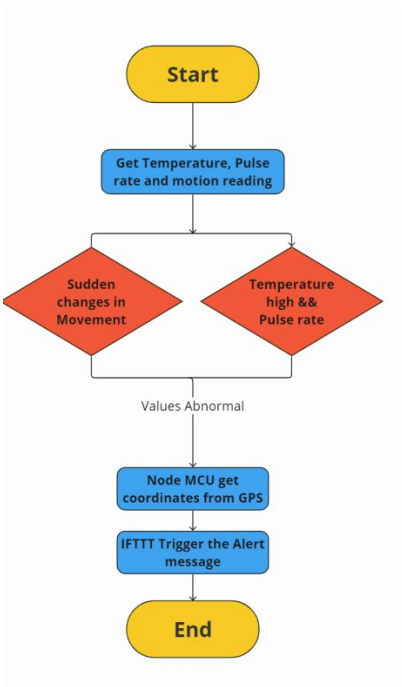

Fig 5.2: Flowchart for Automatic mechanism

Both techniques meet on the alarm instrument, vital for incite help. Figure 5.3 outlines the framework design of the alarm instrument. The GPS module acts as a computerized pathfinder, giving exact area information. Coordinates with Google Maps, it produces a clickable interface, advertising quick get to to the user's area. Imperative data expedite is encouraged through IFTTT web hooks, guaranteeing productive and robotized help by activating predefined activities such as informing crisis administrations or sending alarms to the user's back organize.

These techniques collectively frame a energetic and responsive security framework, advertising clients a range of alternatives for guaranteeing their security. The manual component caters to quick and direct user mediation, whereas the mechanized component includes a layer of persistent checking and danger detection. This coordinates approach guarantees a flexible and user-centric framework, enabling clients to explore their environment with certainty.

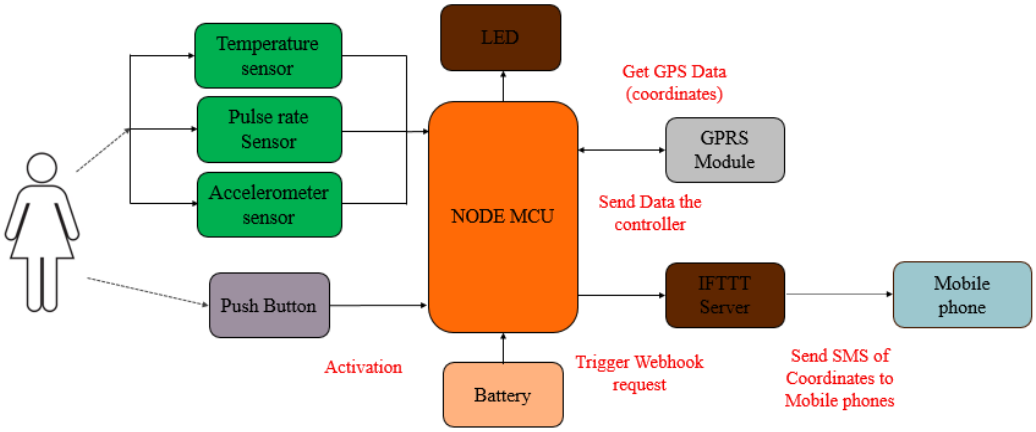

Fig 5.3: System Architecture of Alert mechanism

VI. RESULT AND ANALYSIS

Our system's capabilities and effectiveness are demonstrated through key figures, giving a comprehensive overview of its real-time functions and emergency response mechanisms.

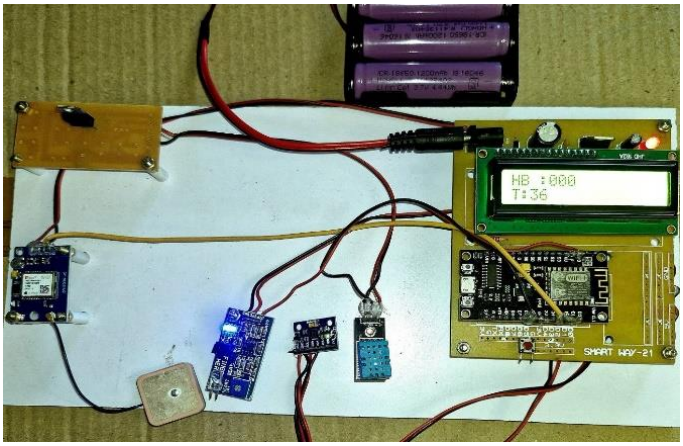

Fig 6.1: Developed device with heart rate and temperature displayed

In Figure 6.1, the developed device with a small LCD screen on the NodeMCU displays real-time data, including the user's heartbeat and surrounding temperature. This immediate insight into the user's physiological state empowers them with valuable information about their well-being.

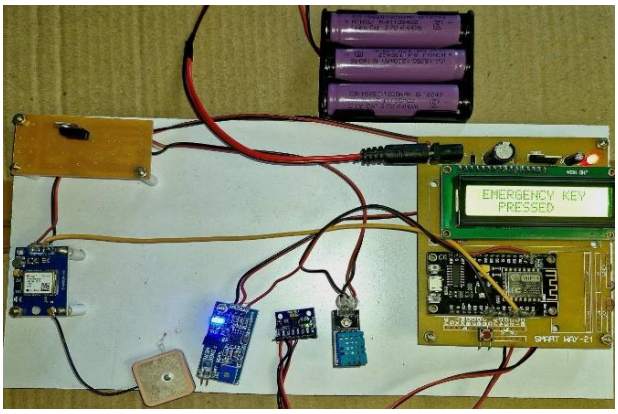

Fig 6.2: Activation of alert mechanism and alert message triggered by IFTTT

.

Figure 6.2 captures a critical moment—the activation of the alert mechanism. The displayed message indicates that the user has pressed the emergency key, showcasing the core functionality of our system. This ensures timely alerts for a swift response in critical situations.

Fig 6.3: SMS received form IFTTT

Figure 6.3 demonstrates the IFTTT webhook in action, with a clickable link embedded within the alert message. This feature coordinates various actions, such as sending notifications to family and law enforcement. The result is a prompt and well-coordinated response during emergencies, enhancing the overall effectiveness of the safety system.

Fig 6.4: Location Tracking in Google Map

Figure 6.4 illustrates the real-time mapping of the IoT device's location. This feature provides an efficient and visually intuitive way to track and locate the user during emergencies. The accuracy of location tracking significantly improves the system's ability to respond promptly and offer assistance in critical scenarios.

These results highlight the practical implementation and success of our safety system, emphasizing its real-time monitoring, alert mechanisms, and efficient emergency response coordination.

VII. CONCLUSION

The progressed framework combines discrete wearables, sensors, cloud foundation, and machine learning calculations to form a energetic security biological system for ladies. The system's execution appeared it is compelling in real-time checking, proactive danger location, and quick reaction. The collaboration between wearables and community sensor observing improves the system's unwavering quality. Furthermore, integration with outside administrations, particularly IFTTT webhooks, guarantees productive and robotized help in basic circumstances. The flexibility of machine learning calculations and user-friendly interface of the portable app contribute to a framework that advances over time and effectively locks in clients in prioritizing their security. The proposed framework successfully progresses women's security by addressing limitations in existing arrangements, employing a flexible and user-centric approach.

VIII. FUTURE WORK

Future work on IoT-based systems for women's safety involves integrating artificial intelligence (AI) algorithms to enhance analytical capabilities, enabling more nuanced threat detection through pattern and anomaly identification in user data. Incorporating voice recognition technology offers an alternative activation method, particularly useful in challenging or hazardous situations. Collaboration with law enforcement and local government is crucial for streamlining emergency coordination, fostering a more effective and informed response. Continuous user feedback and iterative improvements, including firmware and system software updates, are essential to address evolving security needs and enhance user experience. The commitment to embracing emerging technologies, promoting collaboration, and prioritizing user participation ensures the system's evolution into a more robust and responsive solution, contributing to a safer environment for women in various contexts.

IX. ACKNOWLEDGEMENT

The authors are deeply grateful to The Honourable Principal and Faculties of Sri Ramakrishna Institute of Technology, Coimbatore for providing the necessary support, guidance and facilities for the preparation of this paper.

X. REFERENCES

[1]. K. Venkatesh,S. Parthiban,P.Santhoshkumar and C.N.S.Vinothkumar," IoT based Unified approach for Women safety alert using GSM", International Journal of Information & Computation Technology, Volume: 4,pp. 787-792,Jan 2021.

[2]. DhirajSunehra,V. Sai Sreshta,V. Shashank and B.UdayKumar Goud," Raspberry Pi Based Smart Wearable Device for Women Safety using GPS and GSM Technology", International Journal of Electronics and Communication Engineering & Technology(IJECET),Vol: 2, Issue 8, March-April 2020, India.

[3]. A.Helen, M.FathimaFathila, R.Rijwana,Kalaiselvi V.K.G,"A Smart Watch for Women Security based on IoT Concept",2nd International Conference on Computing and Communications Technologies (ICCCT),23-24 Feb 2017, Chennai, India.

[4].Akash Moodbidri, HamidShahnasser," Child Safety Wearable Device",International Conference on Information Networking(ICOIN),11-13 Jan,2017,Da Nang,Vietnam.

[5]. S. Vahini, N. Vijaykumar, "Efficient tracking for women safety and security using IoT", Inter- national Journal of Advanced Research in Computer Science, Volume 8, No,.9, November- December 2017

[6]. HearMe: A Smart Mobile Application for Mitigating Women Harassment", International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), 19-21Dec,2016, Pune, India.

[7].GeethaPratyushaMiriyala, P.V.V.N.D.P.Sunil, RamyaSreeYallapalli, Vasantha Rama Lakshmi Pasam, TejaswiKondapalli ,AnushaMiriyala,"Smart Intelligent Security System for Women", International Journal of Electronics and Communication Engineering & Technology(IJECET),Vol: 7, Issue 2, March-April 2016, pp. 41–46,Andhra Pradesh, India.

[8]. D. Chitkara, N. Sachdeva and Y. Dev Vashisht, "Design of a women safety device," IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Agra, 2016, pp. 1-3.

[9]. Abhijit Paradkar, Deepak Sharma. 2015. All in one Intelligent Safety System for Women Security" International Journal of Computer Applications (0975-8887), 130(11).

[10]. Dhruv Chand, Sunil Nayak, Karthik S. Bhat, Shivani Parikh, Yuvraj Singh, AmitaAjithKamath. 2015. A Mobile Application for Women's Safety: WoSApp. DOI: 978-1-4799-8641-5, IEEE.