

Design and Implementation of Wireless IoT Device for Women's Safety

by

Jannatul Ferdaus Khan Lisa

22141062

Tahsiana Rashid Khan

18101283

Nishat Alam Tuba

18301163

Prioti Saha Tonny

18301211

Md. Shihab Mustafa

21241074

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering

Brac University

May 2022

© 2022. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis submitted is our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Lisa Khan

Jannatul Ferdaus Khan Lisa
22141062

Tahsiana

Tahsiana Rashid Khan
18101283

Md. Shihab Mustafa

Md. Shihab Mustafa
21241074

Tuba.

Nishat Alam Tuba
18301163

Prioti

Prioti Saha Tonni
18301211

Approval

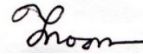
The thesis/project titled “Design and Implementation of Wireless IoT Device for Women’s Safety” submitted by

1. Jannatul Ferdaus Khan Lisa (22141062)
2. Tahsiana Rashid Khan (18101283)
3. Md. Shihab Mustafa (21241074)
4. Nishat Alam Tuba (18301163)
5. Prioti Saha Tonni (18301211)

Of Summer, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on May 24, 2022.

Examining Committee:

Supervisor:
(Member)



Jannatun Noor Mukta
Lecturer
Department of Computer Science and Engineering
BRAC University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Associate Professor
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
BRAC University

Ethics Statement

We conduct research of the highest quality and integrity. The confidentiality and integrity of our research paper contributions are extremely important to us. We conducted our study in an unbiased manner in order to produce an analysis that is independent. Perhaps, in the hereafter, this method of analysis will provide some further benefit to humankind in order for them to progress.

Abstract

As daily newspapers and telecast media gets flooded with rape and murder of young children and women, it becomes a national duty to safeguard their safety at all times. According to a statistic, more than a thousand children and women were raped from between January and October 2020 in Bangladesh. More than 2,700 cases of violence against women and children have been reported, including rape. According to the World Health Organization (WHO), one in three women is a lifelong victim of sexual violence. With the number of atrocities increasing every year, the need to alert someone for help using an advanced system becomes a necessity. A lot of these cases are not considered a serious issue in our country. In this precarious scenario, we propose a device that consists of ESP8266 microcontroller, pulse-oximeter and heart-rate sensor, gps, push button, reset button and a ESP32 wireless camera. The device is connected to the Blynk web server, where it continuously updates the user's pulse-rate and oxygen values. The device is very compact, and can be turned on by pressing the emergency button. It also turns on automatically when the heartbeat and oxygen values rise above the threshold value in case of an emergency. Once the device is turned on, it will send danger alert messages to the necessary contacts and the police station alarming that the girl is in danger. The text message also contains the exact location of the girl using a GPS. In addition, this device is also fitted with a ESP32 wireless camera which snaps a picture of the attacker. To conclude, this device is built based on real life scenario and has the adequate features to guide the women to safety.

Keywords: ESP32 Camera, Emergency Button, ESP8266 nodeMCU, MAX30100 Pulse Oximeter and Heart-Rate Sensor IC for wearable health, Buzzer, Battery, Voltage booster, LED Screen, Stop Button, Cloud Server: Adafruit MQTT, Blynk.

Motivation

Considering, woman's current challenging situations in real life, and the fact that the women atrocity reports keep on rising globally no matter how many steps are taken, motivates us to create something which will ensure their safety and allow them to move freely, a basic human right which they truly deserve. This application strikes a balance between defense abilities and practical real time application.

Acknowledgement

With the blessings of Almighty we finally finished our thesis on the topic "Design and Implementation of Wireless IoT Device for Women's Safety using Machine Learning". It was a learning experience for all of us. We specially acknowledge our honorable supervisor Jannatun Noor miss for her technical support and guidance given, and steering us to successful completion of this work. In honor of our parents, we thank them for their blessings. The Almighty has blessed our efforts with his grace and brought them to a successful conclusion. We have learnt and experienced many important and interesting things throughout this task which will definitely help us in our near future. Our efforts are incomplete without dedicating our gratitude towards everyone who has contributed to our project. Therefore, we would like to thank all the people who has contributed and assisted towards successful completion of our work.

Table of Contents

Declaration	i
Approval	ii
Ethics Statement	iii
Abstract	iv
Dedication	v
Acknowledgment	vi
Table of Contents	vii
Nomenclature	ix
1 Introduction	1
1.1 Research Objectives	2
1.2 Thesis Orientation	3
1.3 Contribution of the Project	3
2 History of IoT and Connected Devices	4
2.1 Survey of related works	5
3 System Designs	11
3.1 Objectives of the proposal	11
3.2 User Driven Design (UDD)	12
3.3 Flowchart	14
3.4 Components Description	16
4 Implementation of the system	22
4.1 Schematic Diagram	22
4.2 Prototype	24
4.3 Code Description	25
4.4 Dataset:	30
5 System Validation	32
5.1 Test 1: Validation of vision functionalities	32
5.2 Test 2: Validation of heart-rate and oxygen reading detection functionality	34

5.3	Test 3: Evaluation of the buzzer notification system	35
5.4	Test 4: Authentication of Blynk web interface and Tasker Application	36
5.5	Summary of Test results	38
6	System Limitations	39
7	Conclusion	41
8	Future Scope	43
	Bibliography	44
9	References	45

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

API Application Program Interface

GPIO General Purpose Input Output

GPS Global Positioning System

GSM Global System for Mobile communication

HCI Human to Computer Interface

HMI Human to Machine Interface

IOT Internet of Things

IP Internet Protocol

MISO Master In Slave Out

MMI Machine Interface

MOSI : Master Out Slave In

OLED Organic Light Emitting Diode

PIR Passive Infrared Sensor

POx Pulse Oximeter and Heart Rate Sensor

RAM Random Access Memory

ROM Read Only Memory

SCLK Serial Clock

UDD User Driven Design

WSD Women Safety Device

Chapter 1

Introduction

The Daily Star published a news on Nov 7, 2021 about a brave girl from Bangladesh, who jumped off a moving bus to avoid being raped. This brave girl was travelling in a bus and could sense imminent danger. When the driver attempted to rape her she jumped of the bus and was saved by another car driver. Just like this scenario, women face immense threat of sexual harassment in the streets, as rapists target them to become their victim. So, their safety is a global issue at the moment. According to a report by Odhikar, a Bangladeshi human rights organization, gang rape cases in the street have nearly tripled from under 100 in 2007 to nearly 300 by the year 2021. In the year 2021 alone, around 3700 women and children in Bangladesh were victims of sexual abuse including rape and murder.

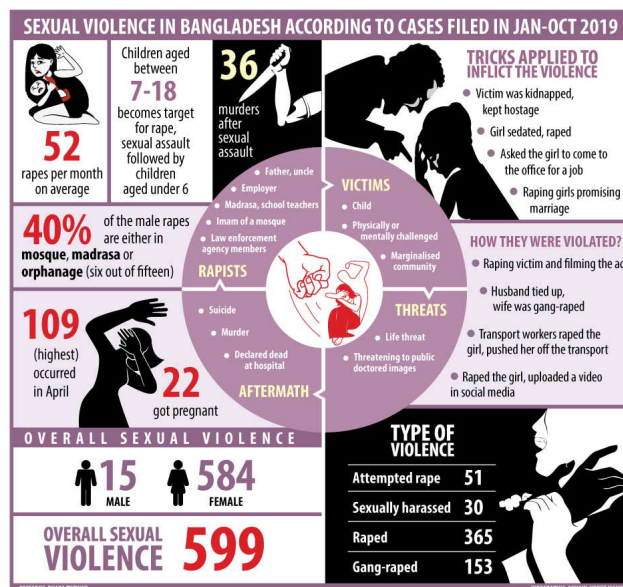


Figure 1.1: Statistics of sexual violence

In today's society, such cases are all too common, which is unacceptable. We need more courageous girls like her who can protect themselves from these criminals. To empower women, we researched in this area and decided to build a safety device which can be used in these kind of scenarios. On the other hand, even if the situation is against her, the device can take action using her vital signs such as heart-beat and oxygen levels. For this, we need a wireless device. That is when

IoT comes for solving the problem, and that is what this research paper focuses on. This paper discusses the functionality of a wireless IoT device that can provide safety for women while they are in any dangerous situation. The devices here can communicate using IoT. The working model here, is a device that sends alerts via text using the GSM cellular method, relay's location coordinates via GPS, and generates an alarm. Wirelessly transferring data from the sensor to a cloud platform which allows monitoring of current data [8]. This equipment is set up to continuously monitor women's vital parameters like pulse rate and temperature [3], and activate automatically if a dangerous scenario arises. It is easy to wear as the material is flexible and non-irritating for the skin and adjustable enough to ensure a comfy fit. This new technology is built in such a way that it serves its purpose to the fullest, which is ensuring women's safety and providing an active lethal form of self-defense.

1.1 Research Objectives

In the last 20 years, Bangladesh has made remarkable prosperity in the sector of women empowerment. According to Dhaka Tribune, the number of working women rose from 16 million in 2010 to 18.5 million in 2016-17. Bangladesh ranked 47th out of 144 nations in 2017 according to the Global Gender Gap Report. Unfortunately as the number of working women continue to rise, so does violence, sexual assaults and rape putting women's security at risk. The horrific rape cases and sexual assaults on women in the streets have shown us that the present crisis cannot be solved by relying solely on the country's law and order. One of the most shocking cases of rape and murder in this scenario is the rape of Shohagi Jahan Tonu who was raped and later murdered in one the most secured place in Bangladesh, military cantonment. While researching on this case we found out that, when Tonu did not return home after tutoring her student, her father started to look for her and unfortunately she was found dead in a devastated condition. Later found out that she was raped before murdered. Even though two autopsies were performed on her and mass protest took place in Bangladesh, we could not bring justice for Tonu. Anyone could blindly say that the case was dismissed by the powerful party. Proper evidence could be the biggest power of any kind of rape case to bring justice. Considering the above cases, we realized that only depending on the laws doesn't solve the problem. We need to take the responsibility of our security in our own hand. Therefore, we decided to build a device that can alert nearby people with a buzzer, send location via message to close one and they can keep an eye by using live-streaming and also save the live for future purpose. Here comes the objective of our device:

- To build a wireless, small and comfortable device that can be easily wearable by girls going outside.
- Choosing appropriate sensors to detect fear or any unexpected situation such as harassment, rape etc.
- To accommodate all the components together we need to choose a suitable microcontroller that can work properly.
- To choose the proper IoT server which will be used for our data management, data collection and so on.

- The device will not only be used as defense system but also to reach out to the family members to locate the victim, preserve evidence via live streaming for future use as well.

1.2 Thesis Orientation

In the following order, we have covered the subsequent chapters. Chapter 2 discusses existing work in this field and history of IoT. Next, Chapter 3 presents the system design of our proposed device, where we introduce you to the components and flowchart in brief. Consequently, Chapter 4, introduces to the implementation of system along with workings with the dataset. Moreover, Chapter 5 contains the system validation. Furthermore, in Chapter 6 we describe the boundaries that we face while working in this project. Lastly, Chapter 7 concludes the paper by summarizing and in Chapter 8 we write about future scope of this device.

1.3 Contribution of the Project

First, we split the tasks between us based on how well each could develop hardware and software as well as write documentation. The software coding part was assigned to Prioti Saha Tonny. The design and implementation of the hardware device was assigned to Nishat Alam Tuba. For documentation, all three authors Jannatul Ferdous Khan Lisa, Tahsiana Rashid Khan and Md. Shihab Mustafa played an equal role.

Chapter 2

History of IoT and Connected Devices

Historically, connected devices date back to 1832, when the first electromagnetic telegraph was developed. These devices communicated directly with each other using electrical signals. In truth, the real history of IoT can be found in the late 1960s, when the internet first appeared which then developed rapidly over the next three or four decades. We have come a long way since those first two machines in the 1980s to the billions of devices we have today. Perhaps it is hard to believe, but the first connected device was actually a Coca-Cola vending machine at Carnegie Mellon University, which was designed by the local programmers. A microswitch and an early version of the internet were used to ensure the drinks were kept cold and Coke cans were in stock. The development of this invention led to further research in the field and the development of interconnected devices all over the world.



Figure 2.1: World's first connected IoT Device

The term "Internet of things" was coined by Kevin Ashton in 1999, thus marking it as one of the most significant dates in the history of the IoT. In a presentation, Ashton discussed IoT as a technology that could connect multiple devices through RFID tags for management of supply chain. In his title, he deliberately used the word "internet" in order to draw the audience's attention, due to the internet's recent popularity at that time. Ashton's breakthrough had a major influence on the development and the history of Internet of Things. In the beginning of the 21st century, the term "internet of things" became popular, with news platforms like The Guardian, the Boston Globe and Forbes mentioning it. Meanwhile, IoT technology was growing in popularity, which resulted in the first International Conference on the Internet of Things held in Switzerland in 2008, with participants from more than 20 countries speaking about RFID, sensor networks and short-range wireless

communications. In addition, several major developments have boosted the IoT evolution. In the year 2000, LG Electronics introduced a refrigerator that could be connected to the internet and allow users to do online shopping and video conferencing. Another important development was the creation of a bunny-shaped robot named "Nabaztag" in the year 2005, which was able to report the latest news, stock market news, and weather forecast. In 2011, there was a big boom in the IoT thanks to its inclusion in Gartner's hype cycle for emerging technologies. IPv6, a network layer protocol that is at the heart of the internet of things, was launched publicly the same year. Since then, interconnected devices have become a part of our daily lives. Companies like Google, Samsung, Apple, Cisco, and General Motors are focusing on the development of IoT sensors and tools from smart glasses to interconnected thermostats, and autonomous cars. Almost every industry in the world like manufacturing, healthcare, transportation, oil energy, agriculture and retail has incorporated IoT in their setup.

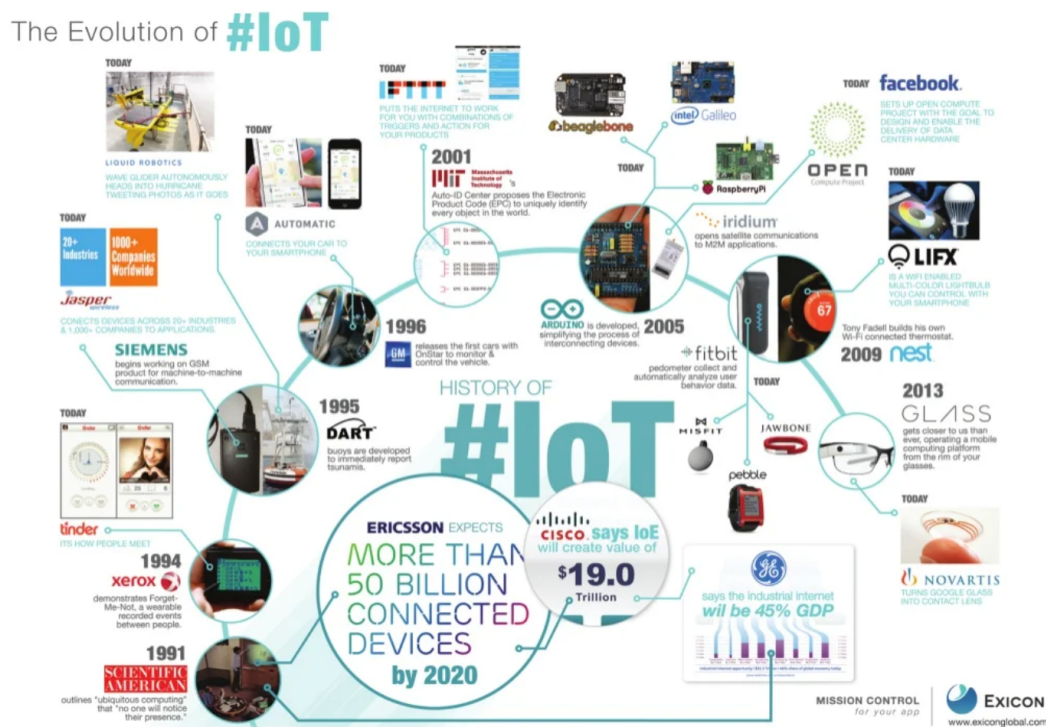


Figure 2.2: The evolution of IoT over the decades

2.1 Survey of related works

The existing women safety system includes wearable devices, smart lockets, smart footwear, smartphone applications and intelligent security systems.

Intelligent System: The authors of paper[1] propose an intelligent women's safety system employing Radio Frequency Identification (RFID) and a Global Positioning System (GPS). Here, the fundamental concept is to combine an active RFID tag with a passive RFID tag. The information is scanned with an RFID reader, and the information is saved. The contacts are passed to the AT89C52 microprocessor. The data bank contains the records of around 4 to 5 persons. When the controller receives data, it sends a message to the appropriate party. GPS is used to track

position. Proteus is used for simulation.

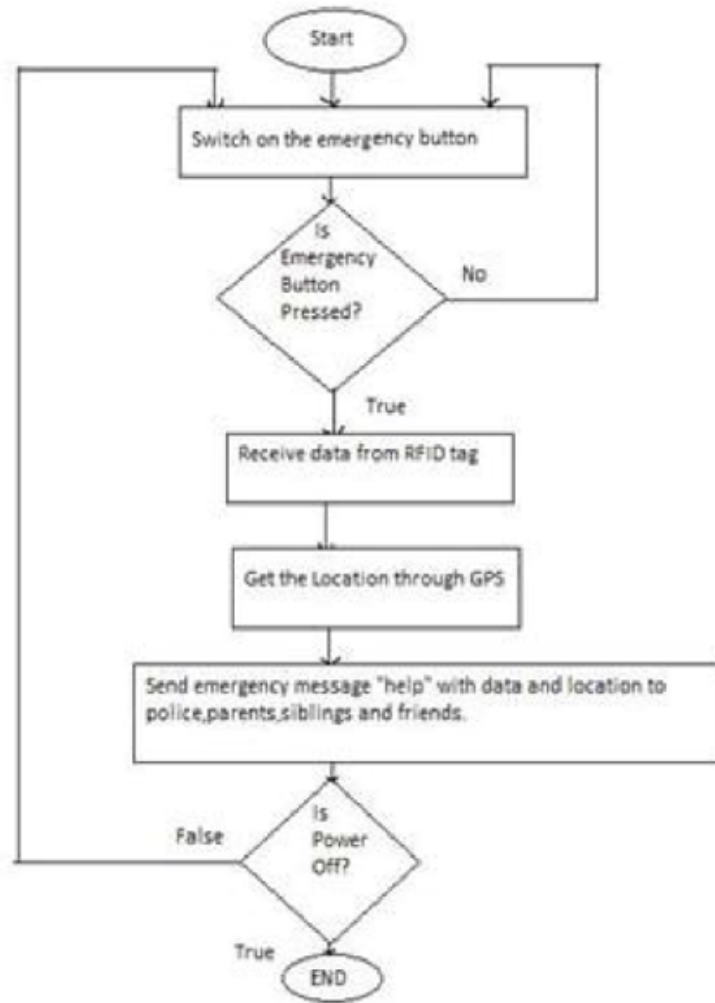


Figure 2.2: Working mechanism of the intelligent system

Smart foot device: In article [2] a smart foot device is created which may be fitted to the buyer's shoes. When activated, this device will send information about the user's location to a smartphone application. The device's downside is that it can also be activated by unintentional foot tapping. For the device to work, the user's foot should be in direct contact with the ground. An alarm is delivered via Bluetooth to a mobile application which is programmed to generate a help message for the user when one foot is four steps behind the other. The Nave Bayes classifier was used to analyze the results. This low-cost gadget had an overall accuracy of 97.5%.

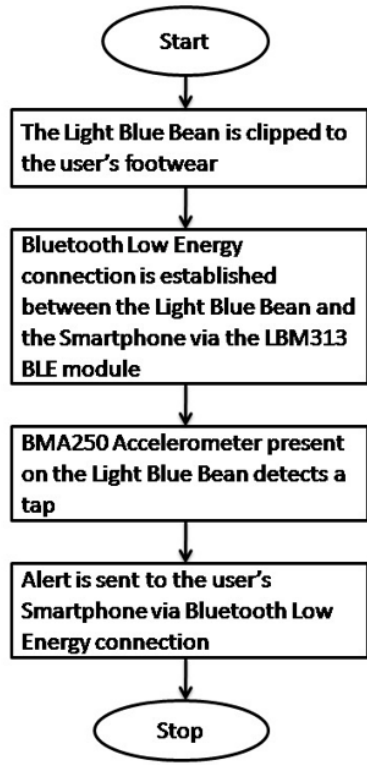


Figure 2.3: Working mechanism of Smart Foot Device

Keep an eye on me: The product is IoT-based that uses a pulse rate sensor to detect whether the victim's pulse rate exceeds a predetermined threshold in a short time. This type of trigger is unreliable since the pulse rate can rise or fall as a result of physical activity. When this system is triggered, the authors of the paper [3] claim that it immediately calls the nearby control room and emergency contacts.

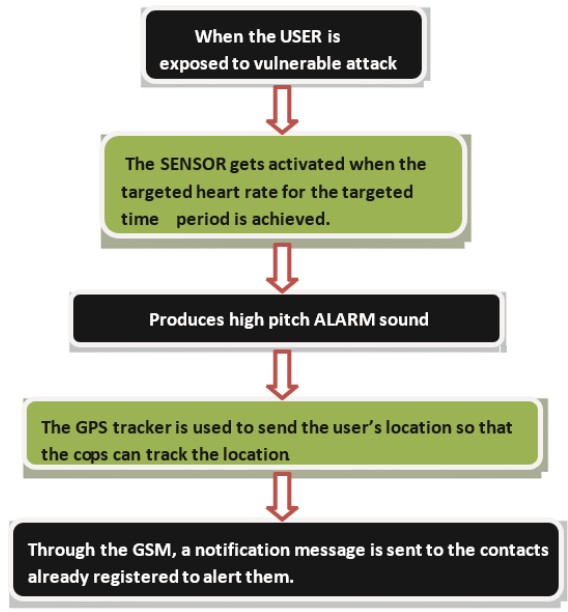


Figure 2.4: Working mechanism of Keep an eye on me

Flex Sensor: The authors of this paper [4] proposed a working model that uses a flex sensor as well as a drop detection sensor. This is unreliable as the user can accidentally turn it on. Live-streaming is initiated with the camera, and the video is transmitted to the control room. The price of the product remains unknown as this model is still in its building phase. The product can be larger than a standard wristband, which might attract unwanted attention.

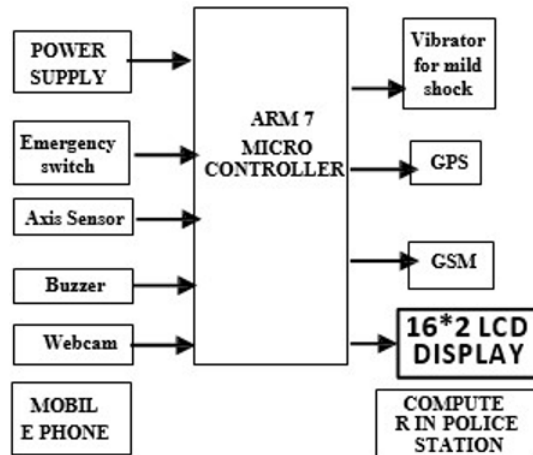


Figure 2.3: Block Diagram of Flex Sensor

Safety Device: This research paper [7] provides a multimodal cost-effective security paradigm for women who may be subjected to offensive risks using deep sensing technologies. Hidden Markov Models (HMMs) provide improved predictive analysis due to their dynamic probabilistic character, and they are useful for developing a dense sensing strategy by analyzing traces of suspicious activity. The use of face recognition and fuzzy labeling of vocal exchanges allows situation-based analysis of relative modeling. In the case of an aftershock, the GSM/GPS module will signal an emergency, otherwise, the female device carrier will receive a notification. Experiments showed that the results were quite promising, with an accuracy of 94.7 percent.



Figure 2.4: Prototype of the device [5]

Alert System: This research paper [7] provides a multimodal cost-effective security paradigm for women who may be subjected to offensive risks using deep sensing technologies. Hidden Markov Models (HMMs) provide improved predictive analysis due to their dynamic probabilistic character, and they are useful for developing a dense sensing strategy by analyzing traces of suspicious activity. The use of face recognition and fuzzy labeling of vocal exchanges allows situation-based analysis of relative modeling. In the case of an aftershock, the GSM/GPS module will signal an emergency, otherwise, the female device carrier will receive a notification. Experiments showed that the results were quite promising, with an accuracy of 94.7 percent.

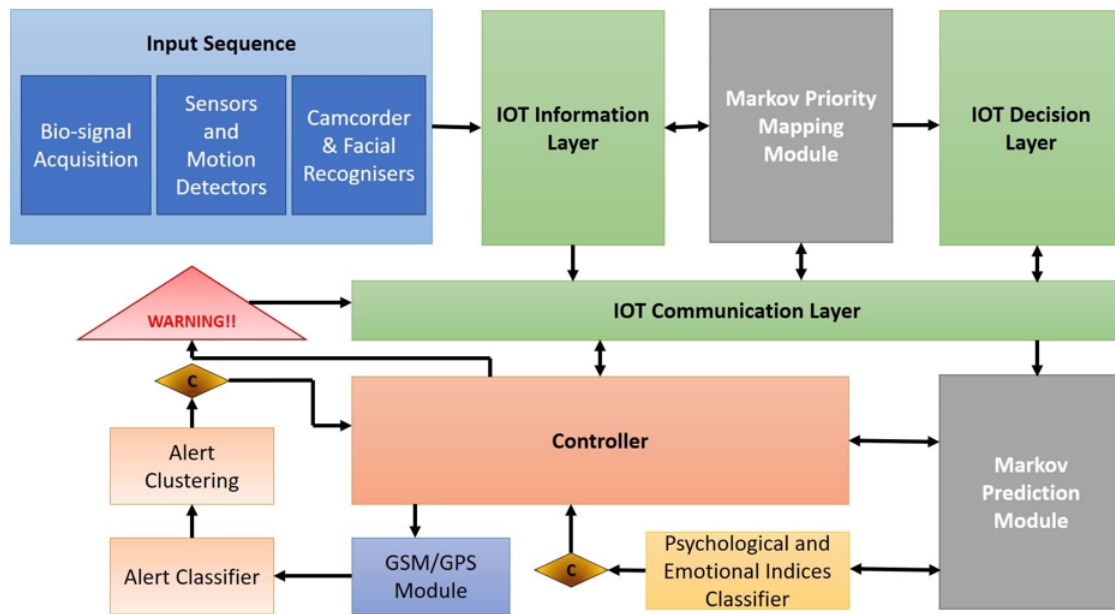


Figure 2.5: Working mechanism of the system [7]

Smart Jewelry: The authors of the study [9] created the Smart Jewelry Bracelet, which is a wearable smart device mounted in a bracelet. It includes an Arduino-compatible Adafruit Flora controller with an accelerometer, gyroscope, pressure and temperature sensors, microphone, and a GPS. The sensors in the smart jewelry bracelet continuously collect data on the user’s activity and vital signs. With Adafruit, a machine learning algorithm recognizes and distinguishes between the user’s typical movements and any abrupt or sudden movements that might indicate an assault. When the bracelet detects an assault, it automatically contacts emergency contacts and pairs with the user’s phone using Bluetooth. The technique can also be used to detect debilitating falls in the elderly. Demonstrations show how the entire process is automated, and the user doesn’t need to be active to seek help from emergency providers. An ordinary fashion bracelet can hold the entire system. This is crucial for ease of use and acceptance. Smart jewelry bracelets provide a viable, cheap and effective way to detect abrupt physical changes in the human body. This smart jewelry bracelet was designed using field-testing and user research. All these features make up this smart jewelry device.

Suraksha: The authors of the paper [10] propose a model named "Suraksha". This is a security system intended specifically for women in crisis. The device is lightweight and easy to carry, and it has a lot of power. To prevent unpleasant situations and offer real-time proof of perpetrators of crimes against women, the primary strategy is to allow victims into providing their location and a distress message to the authorities and a registered phone number. Currently, work is being done to make it smaller so that it may be implanted in jewelry, mobile phones, and other items, making it a more flexible instrument for the public.

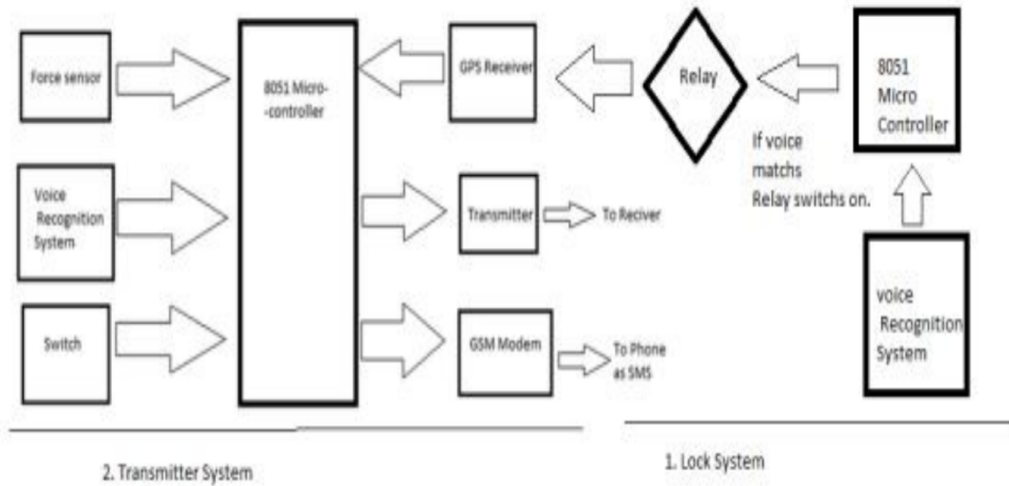


Figure 2.8: Block Diagram of Suraksha[10]

Below is a brief comparison between our device and existing devices in the market.

Technology Used	Name of Paper	User Location & SMS	Live Video Streaming	Alarm	Stop Button for False Alarm	Reliable Data
IoT	Our Paper. (2022)	Yes	Yes	Yes	Yes	Yes
RFID	[1] Shaik et al. (2016)	Yes	No	No	No	Yes
Bluetooth	[2] Nandita et al. (2016)	Yes	No	No	No	No
IoT	[3] Helen et al. (2017)	Yes	No	Yes	No	No
IoT	[4] Sapna et al. (2017)	Yes	Yes	Yes	No	Yes
Machine Learning	[5] Muskan et al. (2018)	Yes	No	Yes	No	Yes
IoT	[6] Saikat et al. (2019)	Yes	No	Yes	No	Yes
Hidden Markov Model	[7] Shreya et al. (2018)	Yes	No	No	No	Yes
IoT	[8] Alisha et al. (2016)	Yes	No	No	No	Yes
Machine Learning	[9] Jayun et al. (2018)	Yes	No	No	No	No
IoT	[10] Nishant et al. (2014)	Yes	No	No	No	Yes

Figure 2.9: Comparison with existing devices.

Chapter 3

System Designs

3.1 Objectives of the proposal

We aim to develop a safety monitoring system to ensure user safety., when she is outdoors. The system should detect abnormal user parameters. (heartbeat and oxygen values). The guardian must be able to watch the user parameters like heartbeat and oxygen values in the Blynk web server and be notified in their mobile device with an alert text message and location in case of an emergency. We assume that the system should consist of the following elements such as ESP8266 microcontroller, ESP-32 camera, buzzer and the Blynk web server, as illustrated in Figure 3.1.

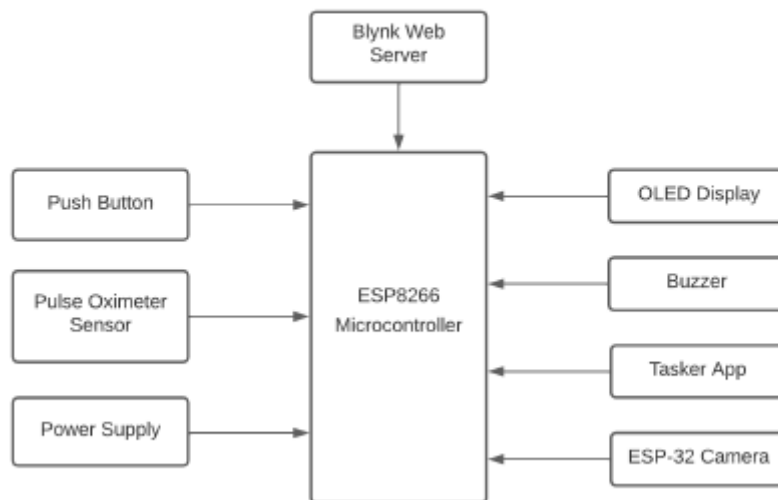


Figure 3.1: Block Diagram of Wireless IoT Device for Women's safety

Pulse oximeter and heart-rate sensor and the ESP-32 camera provides information to the ESP8266 microcontroller. Through the Blynk web server, the ESP8266 communicates with the mobile device of the guardian, who can monitor the user when she is outdoors. Our system is based on the following principles:

- It monitors user parameters (heartbeat and oxygen values).

- If there is any unusual reading, it activates the ESP-32 camera and notifies the guardian via alert text in their mobile device.
- Blynk web server displays the user parameters (pulse-rate and oxygen values) on the interface, which can be accessed by the guardian using their mobile devices.
- The system monitors the user when she is outdoors.

3.2 User Driven Design (UDD)

In User-Driven Design, product development is guided by future users, designers and stakeholders. During the design process, every step is validated with the user. Generally, it is divided into two parts to product development: formulation of a problem and product development.

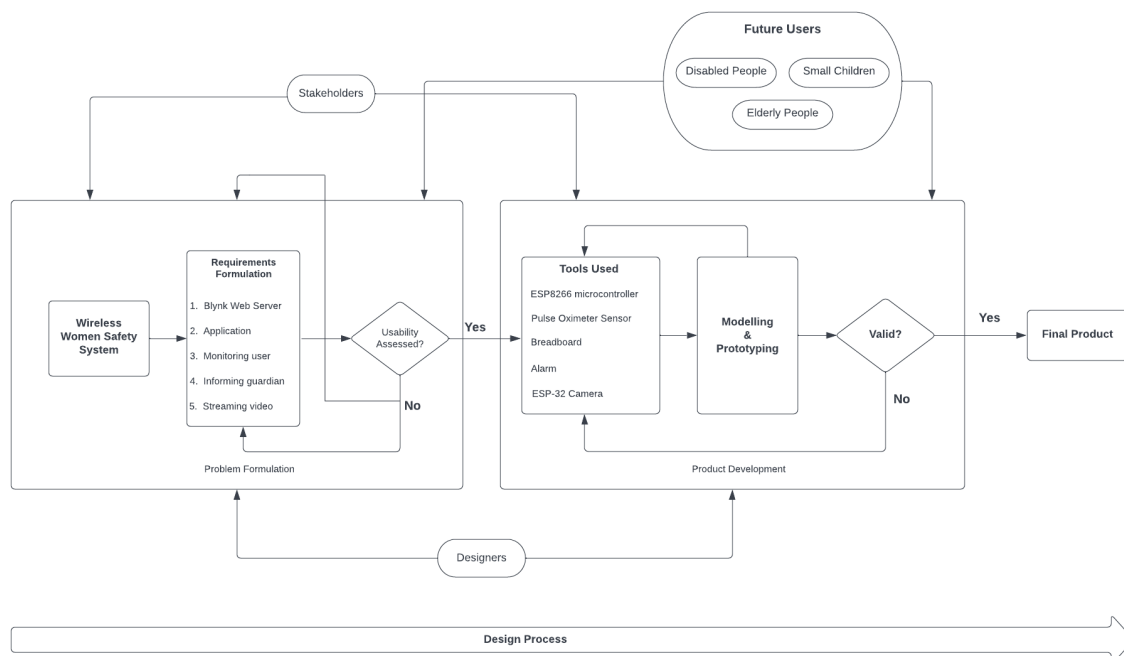


Figure 3.2: User Driven Design Schema

Problem Formulation: Our system would be used by young girls, women and guardians. When the system is implemented, guardians will be able to monitor their users and be alerted if any unusual activity is detected. The guardian can watch live video streaming via the application or web interface. The requirements of the system are user interface, monitoring the user’s activity, and detection of unusual body parameters (heartbeat and oxygen level), see Fig 3.2

Product Development: In order to meet the requirements outlined in the problem description, the following tools are needed: ESP8266 microcontroller, buzzer, ESP32 camera, and pulse and oximeter sensor. Next, flowchart, the block diagram, and schematic diagram should be created for prototyping. Tests must be conducted

after prototyping. Our tests show the system is useful to provide user safety by monitoring user activity that seems unusual. The system can alert the guardian through SMS notification along with the GPS coordinates that the user is in danger and also raise awareness to surrounding people by raising an alarm [19]. Hence, the user-driven design can be seen as a procedure of solving problems in multiple stages. The features of our system are shown in Table 3.2. It covers both general and detailed features and some specific restrictions, as well as some specific restrictions with the related technologies and algorithms

- **Detection of abnormal readings:** The MAX30101 uses an internal LED to reflect light onto arteries and arterioles in the subcutaneous layer of the finger, which is then detected by a photodetector. This process is called photoplethysmography. This data is used by the MAX30101 to determine heart rate and blood oxygen saturation.
- **Monitoring of user, Surveillance, and Face Recognition:** The features listed here are part of the same section. The ESP32 camera is used to monitor the user (user's unusual activities). In addition to video streaming, it can also detect and recognize faces. If the Pulse oximeter and heart sensor detects any abnormal reading, then the ESP32 camera wakes from sleep mode and begins streaming video. The video can be viewed in the user interface.
- **Communication:** The system should be able to alert the user when an alarm condition occurs. The system must be able to communicate with the guardian regardless of the user's location. In case of an emergency, the system should effectively communicate with the guardian by sending alert notifications via text along with GPS location coordinates so that the user can be tracked. Here, the user interface acts as an intermediary between the user and the guardian, storing the user's vital parameters (heart-rate and oxygen values).
- **Interface:** The user interface connects the user to the system. The guardian can access the user data from anywhere and at any time. A web interface and application interface are created. The guardian can access user data and watch video streaming by either logging in to the application or by using a web browser

On the left, you can see the sensors connected to the ESP8266 microcontroller. On the right, you can see the user interface. The central component of the system is the ESP8266 microcontroller, to which three sensors are connected: pulse oximeter and heart sensor, buzzer and ESP-32 camera. The ESP8266 microcontroller controls both input and output in the system. Pulse oximeter and heart sensor is used to detect the heartbeat and oxygen readings. The ESP32-CAM is used to stream video. The buzzer alerts those nearby that the user is in danger of being attacked. When the pulse oximeter and heart sensor detects abnormal heart rate and oxygen values, the user is in danger. The ESP8266 microcontroller will send data regarding the alert to the web interface/application. The web interface allows the guardian to watch video streaming and observe anomalous activity.

Functionalities		Particular Constraints	Used Technologies	Existing Technologies
Detection of readings	< 100Bpm	Validity > 90%	Pulse-Oximeter	PIR Sensor Temperature Sensor Skin Color Sensor
	> 100Bpm	Validity < 70%		
Monitoring of user		High Validity	ESP-32 Camera	Web Camera CMOS
Surveillance		Coverage of user's surroundings	ESP-32 Camera	Web Camera CMOS
Face Recognition		High Validity > 80%	ESP-32 Camera	Nest Hello Mini OV 7690
Communication (Informing guardian)		High Validity > 90%	Blynk Web Server Tasker Application	Bluetooth GSM
Interface		High Validity > 75%	Blynk Web Server	Webpage with domain hosting for security

Figure 3.3: Functionalities table of the Wireless IoT System

3.3 Flowchart

The Pulse Oximeter and Heart sensor are installed in the system, which measures the heart rate and oxygen saturation levels. The readings are passed on to the ESP8266 microcontroller. In case the heart beat and oxygen levels rise above the threshold value, the system raises an alarm. Figure 3.4 represents the flowchart of the system. Based on the readings detected by the Pulse oximeter and heart sensor, the entire process occurs in two ways:

- Pulse Oximeter and Heart-rate Sensor = 1, If the Pulse Oximeter Sensor is active, this means that there is an abnormal heart or oxygen saturation reading above threshold. The buzzer will start ringing. Alert text messages will be sent to the guardian's mobile device via Tasker app. The guardian can watch live video streaming by entering the ESP-32 CAM interface.
- if the Pulse Oximeter Sensor detects normal readings of heartbeat and oxygen below the threshold value, indicating the situation is normal. The values are sent to the Blynk web server and no alarm is raised. The system operates normally.

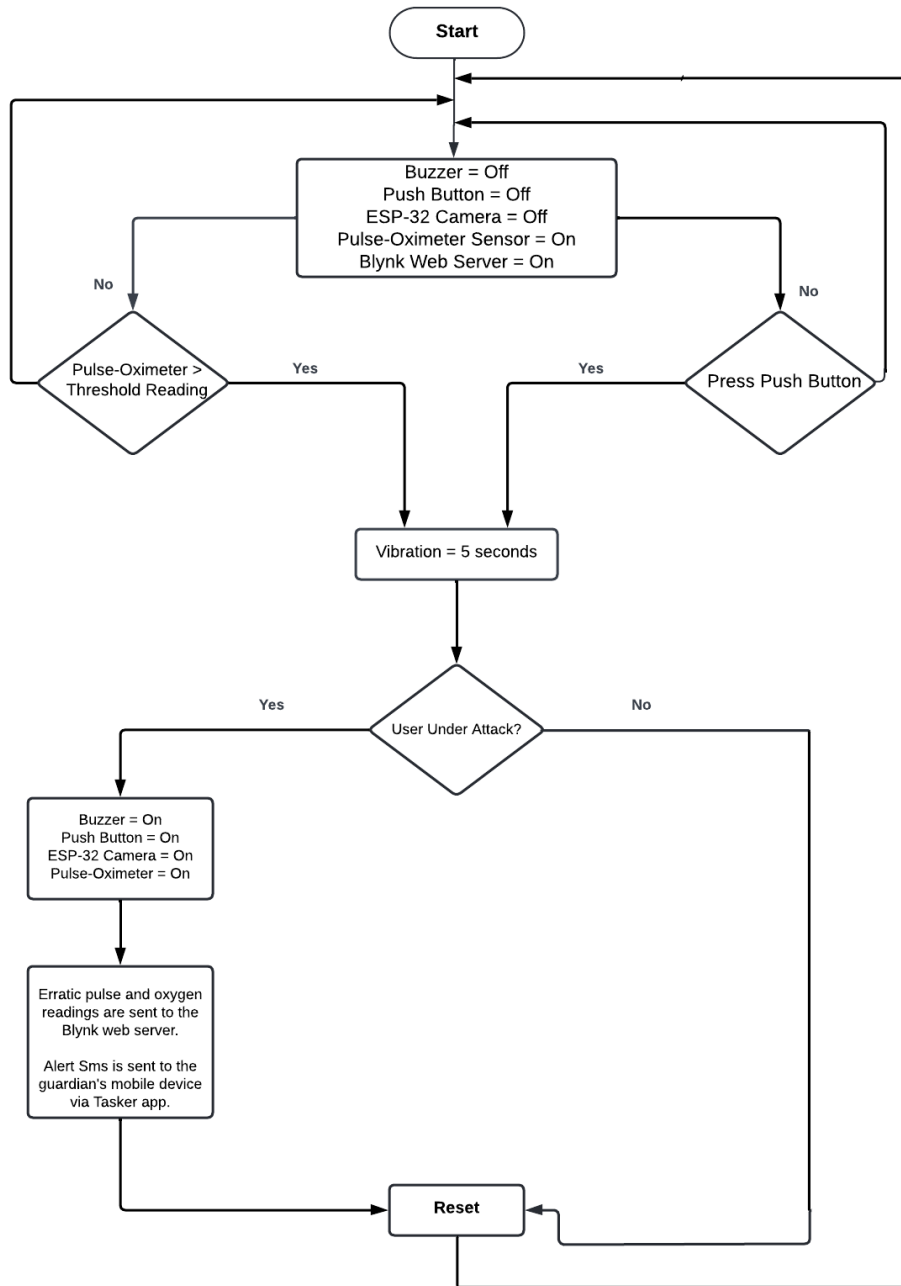


Figure 3.4: Flowchart of the system

3.4 Components Description

ESP8266 microcontroller: The ESP8266 is a low-priced Wi-Fi microprocessor integrated with TCP/IP networking. The ESP8266 microcontroller controls external sensors using its set of GPIO (general purpose input/output) pins, much like other microcontrollers. This microcontroller has 17 GPIO pins, but only 11 can be used. The onboard flash memory chip is accessed by six of the 17 pins. It can also process analog inputs such as voltage levels and convert them to digital values. The ESP8266 can also be connected to a Wi-Fi network, to the Internet, to a web server, and to a smartphone via Wi-Fi.

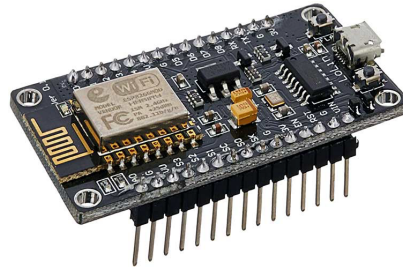


Figure 3.5: ESP8266 microcontroller

- The Pins 1(TX) and 3 (Rx): Receiver (Rx) pin and Transmitter (TX) pin are used to receive and transmit serial data.
- Pins 4(SDA) and 5(SCL): The Serial Data (SDA) pin allows master and slave devices to exchange data. While, Serial Clock (SCL) pins are used to generate synchronized clocks between master and slave devices. 12 (MISO): The Master In Slave Out pin allows the master to receive data and the slave to transmit data.
- Pin 13 (MOSI): The Master Out Slave In pin allows the master to transmit data and the slave to receive data
- Pin 14 (SCLK): This is the Serial Clock pin. It is the Master who generates this clock, which the slave uses for communication. The master can only begin a serial clock.
- Pin 15(CS): This is the Chip Select pin. Using this pin, the Master selects the slave device and begins communicating with it.
- Pin 16 (WAKE): This pin is used to wake up a microcontroller from deep sleep mode.
- Reset pin: It is used to reset the microcontroller.

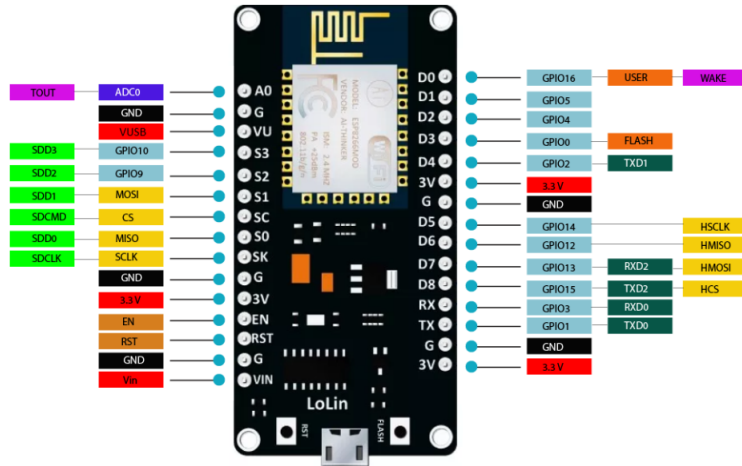


Figure 3.6: Ports Description of ESP8266 microcontroller

ESP32-CAM: The ESP32-CAM is a small, low-power camera module. It comprises a 2-megapixel OV2640 camera that measures 40 mm x 27 mm x 5 mm. There is a micro SD card slot, which is used to save the images shot by the ESP32-CAM.



Figure 3.7: ESP32 CAM Module

The internal memory of the ESP32 camera consists of:

- 448 KB ROM for boot and primary functions
- 520 KB on-chip SRAM for data and commands
- Embedded Flash: The ESP32 CAM has 39 digital pins in total, four of which are inputs. The device supports 18 ADC's of 12-bits and 2 DAC's of 8-bits. The ESP32 ports are depicted in the figure below.

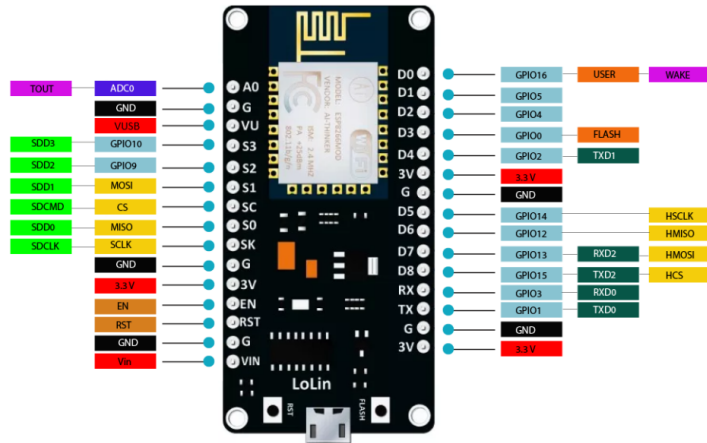


Figure 3.8: ESP32 CAM Ports Description

ESP32-CAM is well suited for IoT applications including smart devices that upload images, facial recognition, video monitoring, etc. The ESP32 has built-in Wi-Fi and Bluetooth modules. The Wi-Fi assigns the IP address. The figure below shows the settings for web streaming for this camera module when connected to the ESP8266.

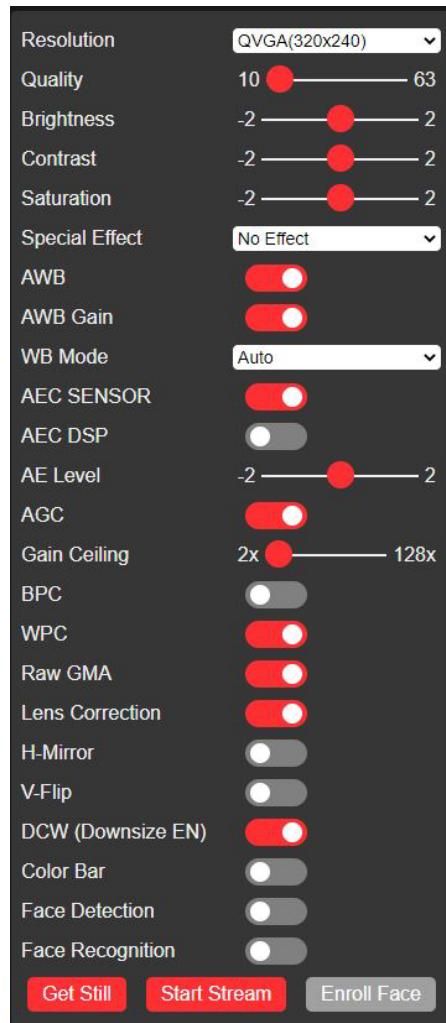


Figure 3.9: ESP-32 Camera Settings

Pulse Oximeter and Heart-rate Sensor: The MAX30101 Pulse Oximeter and Heart-rate Sensor measures the blood oxygen and heart rate of the user. The OLED displays the BPM (pulse rate) and SpO2(blood oxygen level) on the screen.

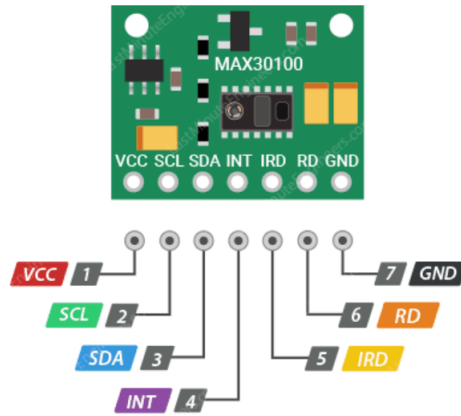


Figure 3.8: Pulse Oximeter Sensor Pinout

The MAX30101 consists of a photodetector, low-noise analog signal processing, optimized optics, and two LEDs to measure heart-rate and pulse oximetry. It works between the range of 1.8V and 3.3V power supply. The MAX30101 uses two lights to shine on the finger or earlobe and measures the amount of light reflected by the object.

Buzzer: The buzzer is an integrated electrical device that emits an alert sound to notify surrounding people. They fall under three categories: piezoelectric, mechanical, and electromechanical. Based on the type of noise they emit, they are categorized. The figure below demonstrates a typical piezoelectric buzzer used in our prototype. It operates at 3V - 16V DC. It has a frequency range of 30Hz - 65500 Hz and can vary from device to device.



Figure 3.9: A typical Buzzer module

Blynk IoT: The Blynk IoT platform controls Arduino, NodeMCU and Raspberry Pi from Android and iOS smartphones through the Internet. With the introduction of Blynk, thousands of deployed IoT products can be connected to the cloud and managed. Blynk automatically saves all data sent from hardware and the data can be accessed only through the application. Blynk is very reliable both for development and personal use. It is free to use, and the Blynk community offers support if you encounter a problem.

In our research, we use the Blynk IoT to store the pulse and oxygen readings of the user, from where it can be retrieved for later use. The pulse and oxygen readings are continuously updated allowing real-time monitoring of the user. The guardian can access the Blynk IoT and monitor the user parameters continuously to see if the user is in danger.

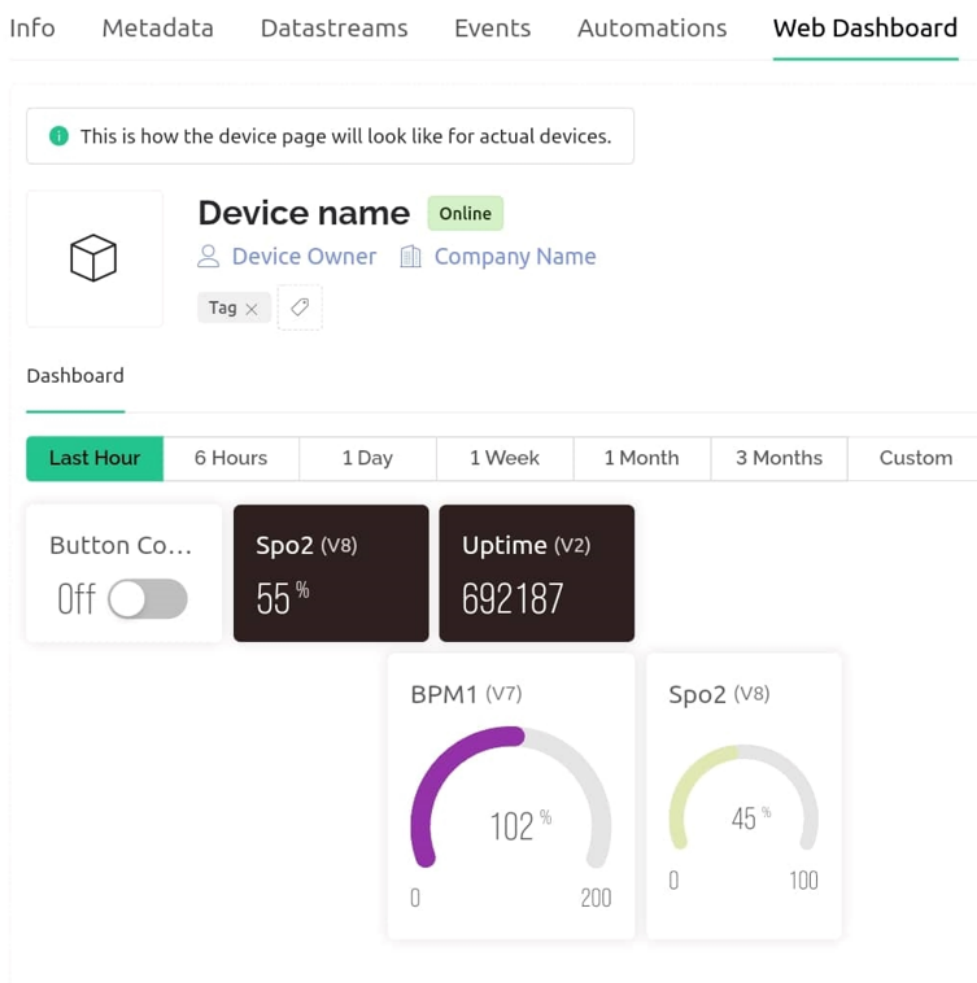


Fig 3.10: Blynk IoT Interface

Tasker App: Tasker is an Android application which does specific tasks based on user input. It is activated by clicks and in our case scenario, a push button. Tasker is an automation app. Here, the user defines a task, which can then be executed based on a variety of contexts. So, it is the user who tells the Tasker what to do. Tasker can also carry out multiple operations on a smartphone. Even before Android had Do Not Disturb mode, Tasker made sure the phone did not disturb as the user slept. During work time, Tasker would automatically switch off the phone to silent mode. While driving, Tasker recognizes the scenario the user is in, and automatically turns off the ringtone to avoid distracting the user.

In our use case scenario, the Tasker app is used to send the alert text message to the mobile device of the guardian to inform that the user is in danger. We use Tasker app because it is cheap to deploy, it only cost us 300TK to setup the whole configuration. Since SIM cards cannot be directly installed in our safety device due to government rules, we had to take Tasker as the cheapest alternative to establish connection with the guardian's mobile device.

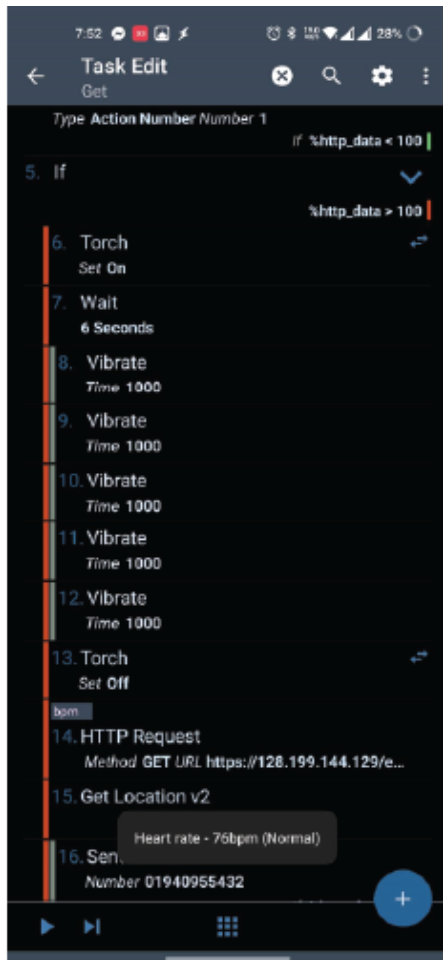


Fig 3.11: Safe condition in the application



Fig 3.12: Alarm activation condition

Chapter 4

Implementation of the system

The chapter comprises two parts, including a description of the hardware and a description of the software. The hardware section describes how the hardware is implemented and validated. The implementation section discusses the modules used in the system, whereas the validation section verifies its functionality. There are two parts to the software description: a description of the code and a description of the application.

In this section we explain the implementation of the system by showing the schematic diagram, the components used in the prototype, along with the description of each component.

4.1 Schematic Diagram

Fig. 4.1 schema diagram illustrates the connections between the ESP8266 and the other components such as camera module, heart sensor, oxygen sensor and the buzzer, where the symbols are denoted as follows:

- SG1 denotes buzzer.
- GND denotes ground.
- VIN denotes input voltage.
- TX denotes transmitter pin.
- Rx denotes receiver pin.

The ESP8266 is connected to the following components. Connection of the ESP8266 microcontroller with the computer:

- ESP8266 microcontroller is connected to the computer using a USB cable type A/B, and the reset pin of the ESP8266 is connected to its ground pin.

ESP8266 microcontroller pins for connecting the ESP32 camera:

- The VCC pin of the ESP32 camera is connected to the 5V pin of the ESP8266 microcontroller, and the ground pin of the ESP32 camera is connected to the ESP8266 ground pin.

- Ground pin of the ESP8266 microcontroller is connected to the D01 pin of the ESP 32 camera.
- Ground pin of the ESP8266 microcontroller is connected to the D01 pin of the ESP 32 camera.
- The transmitter pin (TX) of the ESP32 camera is connected to the transmitter pin of the ESP8266 microcontroller.

Connection pins of ESP8266 microcontroller with the buzzer:

- The 8th digital pin of the ESP8266 microcontroller is connected to the positive pin of the buzzer.
- The ground pin of the ESP8266 microcontroller is connected to the ground pin of the buzzer.

Connection pins of Pulse Oximeter and Heart-rate sensor with the ESP8266 microcontroller

- The VCC pin of Pulse Oximeter and Heart-rate sensor is connected to the 5V pin of the ESP8266 microcontroller
- The ground pin of the Pulse Oximeter and Heart-rate sensor is connected to the ground pin of the ESP8266 microcontroller.
- The Doubt (digital out) pin of the Pulse Oximeter and Heart-rate sensor is connected to the digital 2nd pin of the ESP8266 microcontroller.

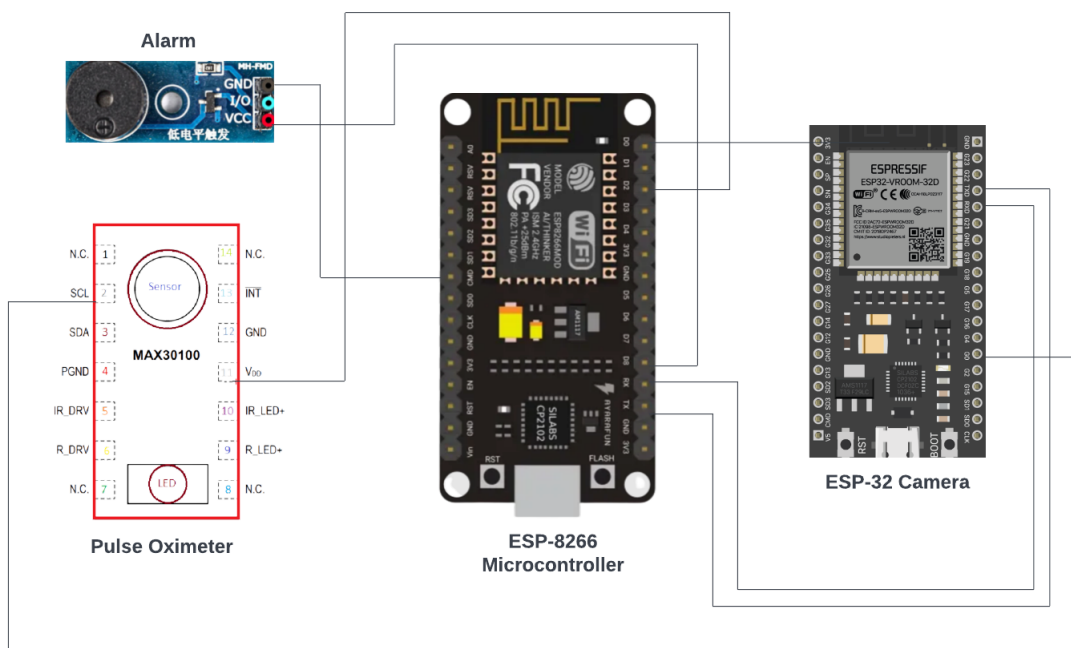


Figure 4.1: Schematic diagram of the system

4.2 Prototype

The figure shows the system design and the connections between the ESP8266 microcontroller and other components (e.g: ESP32-camera, PIR sensor, buzzer). Depending on the needs of the user, it can easily be installed in any room in a house. The necessary conditions for installing the prototype are:

- An Internet connection is required.
- A power supply is needed

This operating model below in Fig 4.2 illustrates the structure and functionality of the women safety system. In the figure below, we explain the working mechanism of the women's safety device. The figure illustrates all the components involved in the system and how they engage with the user through the Blynk web interface and Tasker app.

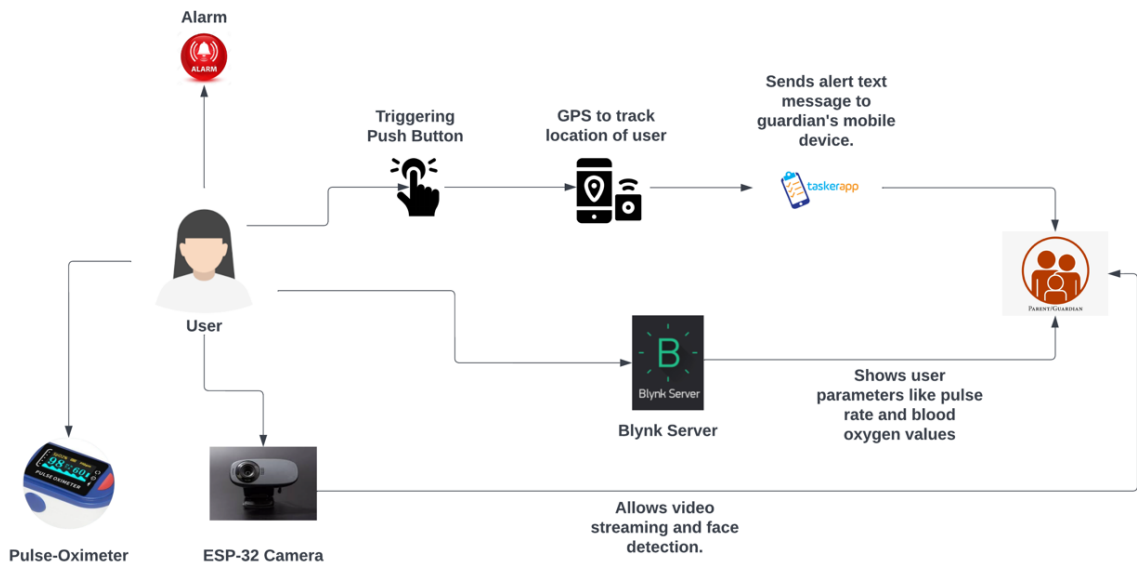


Figure 4.2: Operational Mockup of the Women Safety System

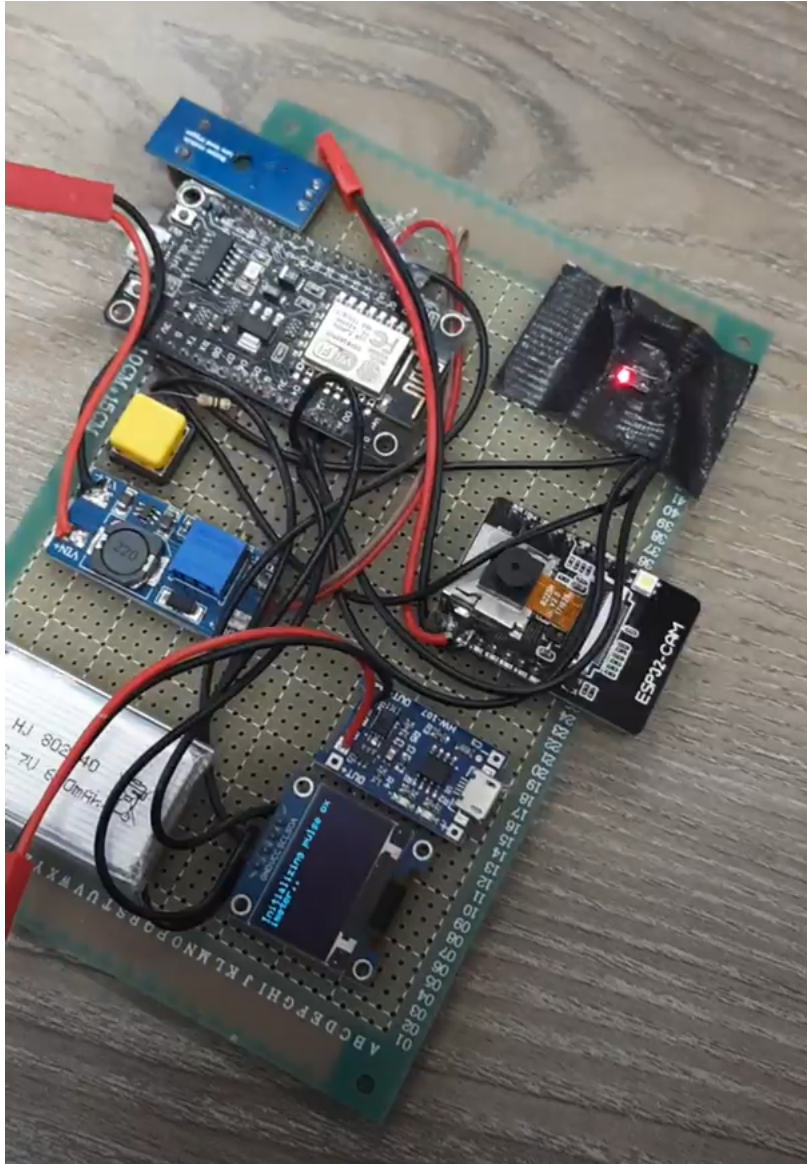


Figure 4.3: Prototype of Women Safety Device

4.3 Code Description

A very important part of this project is coding. The first part is the ESP32-CAM code. In order for this code to work, network credentials must be added, to establish a connection between the system and the network. It is necessary to create an IP address to ensure the program runs as shown in Fig 4.4.

The following part of the code defines the libraries that are imported for various components of our system. These components include the Blynk app (web server where user parameters of heartbeat and oxygen values from pulse-oximeter and heart-rate sensor are stored), ESP8266 microcontroller, pulse-oximeter and heart-rate sensor(MAX30100), wire, and OLED (for display).

As soon as the network credentials are entered, the system connects to the network and the entire process starts operating, and the IP address is displayed on the screen. To see the entire process, we need to run the code as shown in Figure 4.6.


```
// Your WiFi credentials.  
char ssid[] = "DecSec ^_^";  
char pass[] = "PmzQ#234&zZz";
```

Figure 4.4: Data for connecting mobile hotspot

```
#define BLYNK_TEMPLATE_ID "TMPLiFN4-2CY"  
#define BLYNK_DEVICE_NAME "Quickstart Template"  
#define BLYNK_AUTH_TOKEN "hAw7W9VvL1Z0YJrAsqsar4ATnEaZDu3q"  
#include <Wire.h>  
#include "MAX30100_PulseOximeter.h"  
#define BLYNK_PRINT Serial  
#include <Blynk.h>  
#include <ESP8266WiFi.h>  
#include <BlynkSimpleEsp8266.h>  
#include "Wire.h"  
#include "Adafruit_GFX.h"  
#include "OakOLED.h"  
#define REPORTING_PERIOD_MS 1000
```

Figure 4.5: Libraries imported for various components in the system



```
esptool.py v2.6-beta1  
Serial port COM10  
Connecting.....
```

Figure 4.6: ESP-32 Camera Results

When the setup is complete, we can see the “ Ready to stream” dialog in the output console. If the pulse-oximeter sensor receives normal heart and oxygen readings, then the OLED screen shows the specific reading detected. If the pulse-oximeter and heart-rate sensor detects abnormal pulse oxygen values above the threshold value, then the OLED screen starts blinking and after 5 seconds starts off the alarm. After that, the alert text message is sent along with the location to the predefined contacts (guardian). The picture of the OLED screen in the system is shown in Figure 4.7.

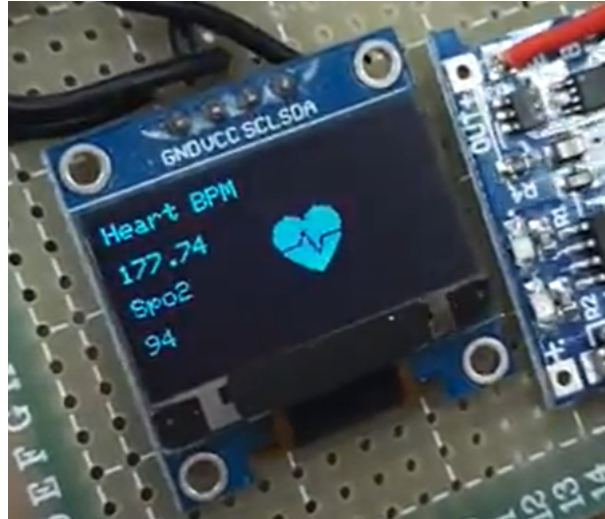


Figure 4.7: OLED Screen

Web interface and application: An interface is a type of medium between ports, for example, the channel between users and the system. Users can get data at any location and time via the web interface. The web interface helps users create, command, or modify systems. The hand tip can be used at home or remotely.

There are a variety of ways in which interfaces can be further categorized, such as Human-to-Machine Interface (HMI) and Human-to-Computer Interface (HCI). Connecting the users and the system from remote areas is the primary goal of the web interface.

Unlike gateways and access points, which contain control panels, routers provide access by entering the IP address to the web browser in order to access the interface. In our system, we used the Blynk web interface to connect the user (girl) and the guardian. In interfacing, this prototype falls under the category of Human-to-Computer Interface (HCI). This interface allows the guardian to monitor her child using their mobile phone and track to see if they are in danger by monitoring the heartbeat and oxygen values, and also opening the camera if necessary. Various types of interfaces are available, including Bluetooth, IP address connections, and APIs or Application Program Interfaces. In our working model, we used API and IP address connections. By entering the IP address in the web browser, the user will be able to access the heartbeat and oxygen values via the Blynk web interface and watch video streaming using the ESP-32 camera.

The application that we implemented in our project is a Wireless Safety Device for Women. The users must download and register the Tasker app on their mobile de-

vice. This app acts as a communication medium between the user and the guardian. The Tasker app fetches the data from the Blynk web interface and sends the data to the guardian's mobile phone. In order for this to work, the guardian must log in to the system using the Wi-Fi credentials (SSID and password). The guardian can access the user's parameters (heartbeat and oxygen values) by logging in to the Blynk web server. In case of an emergency, the guardian is immediately notified with alert messages via text messages (through the Tasker app) showing the exact location of the user. The guardian can watch video streaming by simply opening our custom-made website and clicking the start streaming option. The streaming can also be turned off manually. Through this application, the guardian can monitor her child's whereabouts and be notified in case of an emergency. The coding required to build the application interface is shown in Figures 4.8, Figure 4.9.



```
Done.ino | Arduino 1.8.19 (Windows Store 1.8.57.0)
File Edit Sketch Tools Help

Done.ino
#define BLYNK_TEMPLATE_ID "TMPLiFN4-2CY"
#define BLYNK_DEVICE_NAME "Quickstart Template"
#define BLYNK_AUTH_TOKEN "hAw7W9VvL1Z0YJrAsqsar4ATnEaZDu3q"
#include <Wire.h>
#include "MAX30100_PulseOximeter.h"
#define BLYNK_PRINT Serial
#include <Blynk.h>
#include <ESP8266WiFi.h>
#include <BlynkSimpleEsp8266.h>
#include "Wire.h"
#include "Adafruit_GFX.h"
#include "OakOLED.h"
#define REPORTING_PERIOD_MS 1000
OakOLED oled;
```

Figure 4.8: Picture of coding with library imports shown

The coding for the application is written in Arduino IDE. The first step in coding is defining libraries such as wire, adafruit, Oak OLED, Blynk app, Pulse Oximeter, ESP8266 microcontroller to gain access to all their associated functions. To create the application, we created a class that contains functions including onBeatDetected and bitmap.



```

const unsigned char bitmap [] PROGMEM=
{
0x00, 0x00, 0x00, 0x00, 0x01, 0x80, 0x18, 0x00, 0x0f, 0xe0, 0x7f, 0x00, 0x3f, 0xf9, 0xff, 0xc0,
0x7f, 0xf9, 0xff, 0xc0, 0x7f, 0xff, 0xff, 0xe0, 0x7f, 0xff, 0xff, 0xe0, 0xff, 0xff, 0xff, 0xf0,
0xff, 0xf7, 0xff, 0xf0, 0xff, 0xe7, 0xff, 0xf0, 0xff, 0xe7, 0xff, 0xf0, 0x7f, 0xdb, 0xff, 0xe0,
0x7f, 0x9b, 0xff, 0xe0, 0x00, 0x3b, 0xc0, 0x00, 0x3f, 0xf9, 0x9f, 0xc0, 0x3f, 0xfd, 0xbf, 0xc0,
0x1f, 0xfd, 0xbf, 0x80, 0x0f, 0xfd, 0x7f, 0x00, 0x07, 0xfe, 0x7e, 0x00, 0x03, 0xfe, 0xfc, 0x00,
0x01, 0xff, 0xf8, 0x00, 0x00, 0xff, 0xf0, 0x00, 0x00, 0x7f, 0xe0, 0x00, 0x00, 0x3f, 0xc0, 0x00,
0x00, 0x0f, 0x00, 0x00, 0x00, 0x06, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
};

void onBeatDetected()
{
  Serial.println("Beat Detected!");
  oled.drawBitmap( 60, 20, bitmap, 28, 28, 1);
  oled.display();
}

```

Figure 4.9: Picture of coding with functions shown

```

void setup() {
  pinMode(D6, OUTPUT);
  pinMode(D5, INPUT);
  noTone(D6);
  Serial.begin(115200);
  oled.begin();
  oled.clearDisplay();
  oled.setTextSize(1);
  oled.setTextColor(1);
  oled.setCursor(0, 0);

  oled.println("Initializing pulse oximeter..");
  oled.display();

  pinMode(16, OUTPUT);
  Blynk.begin(auth, ssid, pass);

  Serial.print("Initializing Pulse Oximeter..");
}

```

Figure 4.10: Setup of pins in the system

4.4 Dataset:

Using a woman's heart rate and oxygen values, this gadget can determine whether she is in danger or not. If she is in danger, it will instantly notify the relevant people. This paper employed the "Logistic Regression" Machine Learning technique to make predictions. Pulse rate and oxygen values will be collected by the machine learning algorithm. The program will then perform computations and generate graphs for both the training and testing data sets. As depicted in the figure below, we used more than 2,000 readings for training and testing.

```
1 pulse_temperature_data['Result'].value_counts()
Normal      2164
Abnormal    126
Name: Result, dtype: int64
```

In total, 2164 readings are normal and 126 readings are abnormal. However, the dataset was highly unbalanced, so we followed the procedure of "Under Sampling" and broke down the entire dataset into normal readings and abnormal readings. Here is a comparison of both the values of normal and abnormal readings.

```
1 # compare the values for both transactions
2 pulse_temperature_data.groupby('Result').mean()
```

	ID	Oxygen	PulseRate
Abnormal	850.523810	92.476190	102.992063
Normal	1161.616913	92.640943	99.856747

Then we concatenated the two data frames in a new dataset and named it "new dataset".

```
1 new_dataset = pd.concat([Normal_sample, Abnormal], axis=0)
```

Then we split the data into training and testing data and applied "logistic regression" method to predict the accuracy of data.

```
Model Training
Logistic Regression

[143] 1 model = LogisticRegression()

[144] 1 # training the Logistic Regression Model with Training Data
      2 model.fit(X_train, Y_train)

LogisticRegression()
```

Using Logistic Regression, we calculate the accuracy of training and testing data. The accuracy of training data is 94.49% and accuracy of testing data is 94.54%.

Model Evaluation

Accuracy Score

```
[145] 1 # accuracy on training data
      2 X_train_prediction = model.predict(X_train)
      3 training_data_accuracy = accuracy_score(X_train_prediction, Y_train)
```

```
[146] 1 print('Accuracy on Training data : ', training_data_accuracy)
```

```
Accuracy on Training data : 0.9448689956331878
```

```
[147] 1 # accuracy on test data
      2 X_test_prediction = model.predict(X_test)
      3 test_data_accuracy = accuracy_score(X_test_prediction, Y_test)
```

```
[148] 1 print('Accuracy score on Test Data : ', test_data_accuracy)
```

```
Accuracy score on Test Data : 0.9454148471615721
```

Chapter 5

System Validation

The test results from the various validation and verification tests are discussed in this section, along with an analysis of the results.

5.1 Test 1: Validation of vision functionalities

Aim: To check the functionality of the vision system.

Components: ESP8266 microcontroller, ESP32 Camera and Blynk Web interface

Objectives: The goals of using this ESP32 camera are as follows:

- checking the resolution of the video.
- verifying the range of ESP32 cameras.
- checking the accuracy of the live video streaming in the user interface.
- checking the ability to stream black/white.

Procedure: The procedure is explained in the following steps:

- Establish a connection between the ESP32 camera and the ESP8266 microcontroller. The connections are as follows: A 5V pin of ESP8266 connected to VCC pin of ESP32 camera and ground pin of ESP8266 connected to the ground pin of ESP32 camera. The ground pin of ESP8266 is connected to the D01 pin of the ESP32 camera. The transmitter pin (TX) of ESP32 camera is connected to the transmitter pin of ESP8266, and the receiver pin (Rx) of ESP32 camera is connected to the receiver pin of ESP8266 microcontroller.
- Once the connection between the ESP32 camera and the ESP8266 microcontroller is established, the network credentials for the connection between the system and the network (Wi-Fi SSID and password) are typed.
- The range of the ESP32 Camera is estimated (the area that the ESP32 camera can cover when streaming).
- In the user interface, check whether black and white video can be streamed.
- The user interface should display accurate live video streaming.

While conducting the test, the attacker must remain at a distance of 1.5 meters from the camera.

Technical specifications: ESP8266 microcontroller:

- Operating voltage = 3.3 V.
- No digital input/output pins = 17.
- No analog input pins = 6.
- Flash memory = 32 KB.
- CLK Speed = 160 MHz.
- ADC = 10 bits ESP32 Camera
- Clock speed = 160 MHz
- Input Voltage = 5 V
- Camera resolution = 2 MP
- Image Transfer Rate = 15 - 60 fps

Observations: The webcam image is shown in Figure 6.1. We can assess the quality of the video by looking at the picture (the video resolution is 240 HD). The camera is connected to the microcontroller and the web interface using the ESP8266. The user interface offers options for adjusting black and white, negative, and grayscale video streaming. Streaming black and white and white is only possible through the web interface, not through the application.

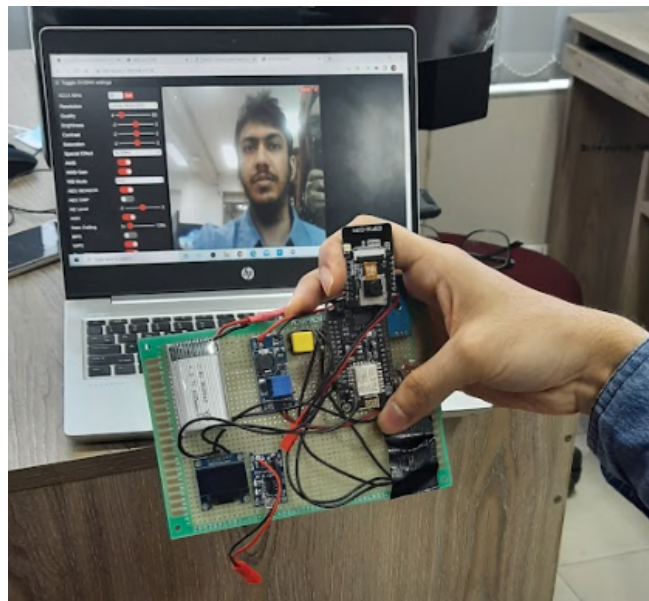


Figure 5.1: ESP-32 Camera results

Results: HD video streaming is of average quality. In the web interface, the settings can be adjusted to enable black and white video streaming. The web camera covers a distance of three meters. Thus, we can conclude that the vision functionality is valid.

5.2 Test 2: Validation of heart-rate and oxygen reading detection functionality

Aim: To examine whether the Pulse Oximeter Sensor is detecting the abnormal readings properly. Components: Pulse Oximeter and Heart-rate Sensor, ESP8266 microcontroller.

Objectives: The Pulse Oximeter and Heart-rate Sensor must be able to detect abnormal heart rate and pulse readings above the threshold value. If the user's heart rate is abnormally high, it should be high (HRT = 1), and if the user's heart rate is normal, it should be low (HRT = 0). Also, we need to check the delay time of the sensor. The delay time is the length of time that the heart sensor remains active after an abnormal heart rate reading is detected.

Procedure: Here is a detailed description of the procedure:

- Connect the Pulse Oximeter and Heart-rate Sensor to the ESP8266 microcontroller. Pulse Oximeter and Heart-rate Sensor positive and negative to the ESP8266 VCC and ground, the sensor pin is connected to the 2nd pin of the ESP8266 microcontroller.
- Give power supply to the ESP8266 microcontroller, and the Pulse Oximeter and Heart-rate Sensor will start working. Write the code inside the ESP8266 microcontroller.
- There are two ways to detect readings. —Case 1: When the pulse readings are normal below 100 Bpm. —Case 2: When the pulse readings exceed 100 Bpm.
- The Arduino IDE will display the status of the Pulse Oximeter Sensor (high, low).
- The delay time is the time the Heart sensor is high after readings are detected.

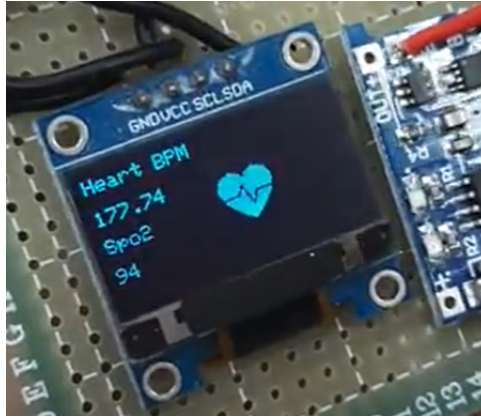


Figure 5.2: Display of BPM and SpO2 readings

5.3 Test 3: Evaluation of the buzzer notification system

Aim: To determine the frequency of the buzzer when it is active and to check the operation of the buzzer associated with the Pulse Oximeter and Heart-rate Sensor.

Components: ESP8266 microcontroller, buzzer, Pulse Oximeter and Heart-rate Sensor.

Objectives: Pulse Oximeter and Heart-rate Sensor should activate the buzzer if abnormal readings far exceed the threshold value are detected.

Procedure: Tests are conducted to determine whether the buzzer is working properly. The following tests outline the procedure in detail.

- Connect the positive and negative of the Pulse Oximeter and Heart-rate Sensor to the ESP8266 microcontroller 5V and the ground. Connect the sensor pin to the second pin. Connect the negative of the buzzer to the ground and the positive pin to the eighth pin. The negative pin of the buzzer should be connected to the ground, while the positive pin should be connected to pin 8.
- Connect the ESP8266 microcontroller to the power supply as described above. Now, the pulse oximeter and heart-rate sensor will start functioning.
- **Case 1:** If the pulse oximeter and heart-rate sensor detect abnormal readings above the threshold value, then record the frequency of the buzzer and its state (high or low).
- **Case 2:** If the pulse oximeter and heart-rate sensor give normal readings, then record the frequency of the buzzer and its state (high or low).

Technical Specifications: Buzzer:

- Operating Voltage = 3V-24V DC.

- Frequency = 3,300Hz.
- Type of Sound = Beep.
- Supply Current = 15mA.
- Operating Temperature = -20 °C to +60 °C.

Observations: The working mechanism of the buzzer is illustrated in Fig 5.3. The sounds could not be shown, however we can see the buzzer activation due to heart and pulse detection. Whenever the pulse oximeter and heart sensor detects abnormal readings in case of an emergency, the buzzer will alert the surrounding people immediately by ringing loudly with a beep sound.

Results: Through this test, we can see if the buzzer is functioning in conjunction with the pulse oximeter and heart-rate sensor. It's on and off conditions. The buzzer is on when anomalous heart and pulse readings are detected, and off when no abnormal heart and pulse readings are detected. In addition to scaring the attacker, the buzzer will also alert surrounding people. Therefore, the usability of buzzer is tested using the experiment.

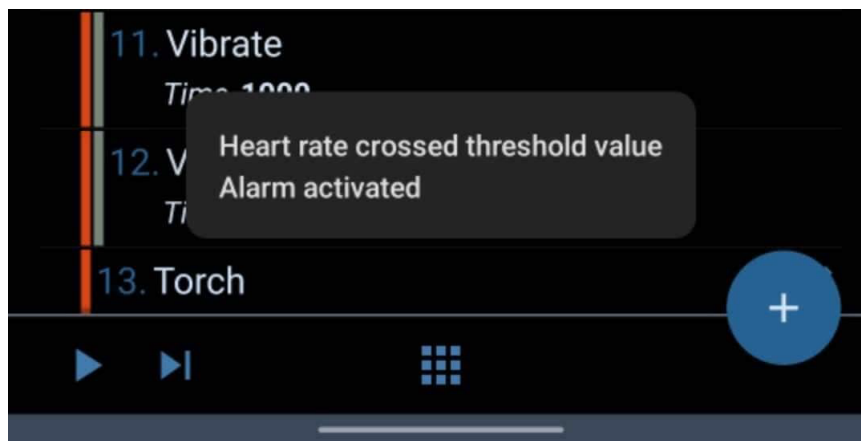


Figure 5.3: Alarm activation after abnormal readings

5.4 Test 4: Authentication of Blynk web interface and Tasker Application

Authentication of Blynk web interface and Tasker Application

Aim: To verify the system's functionalities when all the parts are connected and to check the interface of the system.

Components: Buzzer, pulse oximeter and Heart-rate sensor, ESP8266 microcontroller, ESP32 camera.

Objectives: The test aims to:

- The user interface (application, Blynk web interface) must allow users to access the data.

- In the event of an alert situation, parents/guardians must receive alert notifications (via Tasker app) that their child is in danger.

Procedure: Below is a detailed explanation of the steps.

- ESP8266's 5V pin is connected to the VCC pin of the ESP32 camera, and its ground pin is connected to the ESP32 camera's ground pin. The ground pin of the ESP8266 microcontroller is connected to the D01 pin of the ESP32 camera.
- The 8th digital pin of the ESP8266 microcontroller is connected to the positive pin of the buzzer, and the ground pin of the ESP8266 is connected to the ground pin of the buzzer.
- ESP8266's 5V pin is connected to the VCC pin of the Pulse Oximeter and Heart-rate Sensor. The ground pin of the ESP8266 microcontroller is connected to the ground pin of the Pulse Oximeter and Heart-rate Sensor. The Out pin of the Pulse Oximeter and Heart-rate Sensor is connected to the 2nd digital pin of the ESP8266 microcontroller.
- Compiling the ESP8266 microcontroller code to provide the required credentials for connecting the ESP8266 microcontroller to the network.
- Following the system's connection to the network, its functionality is checked in two ways: Method 1: The Tasker app will display the output "Normal" when the pulse oximeter and heart-rate sensor show normal readings (HRT = 0). Using the Blynk web server, the user interface will show normal heart rate and oxygen readings of the user. Method 2: If the pulse oximeter and heart-rate sensor both indicate they are high, the ESP8266 microcontroller activates the buzzer. The guardian will be notified about the alert by the Tasker application, and the Blynk web browser will show the pulse and oxygen readings. Through the ESP-32 IP address, the guardian can watch the video streaming. Here, the ESP-32 user interface will stream live video.
- The guardian can watch the live stream video without being alerted by the pulse oximeter and heart-rate sensor by logging in the ESP-32 web interface.

Technical Specifications:

- Low-power dual-core 32-bit CPU
- 802.11b/g/n Wi-Fi
- Bluetooth 4.2 with BLE
- Built-in 520 KB SRAM
- External 4 MB PSRAM
- CLK Speed = 160 MHz

Observations: Images corresponding to UI warnings and secure notifications are shown in Figures 5.4 and 5.5 below. If an alert condition exists, the guardian receives an alert message that the user is in danger along with her GPS location coordinates so that the user can be tracked. Starting and stopping video streaming options are available throughout the application interface and web interface, so the guardian can control video streaming.

Results: When all the components are connected to each other, the system works perfectly. Both the application and web interface offer accessibility via their user interfaces. A web interface is not as secure as an application program interface. An alert notification will appear in the user interface if there are abnormal heartbeat or oxygen readings. When the readings are normal, the system updates the guardian that the user is safe.

5.5 Summary of Test results

The tests are run on various components and each test is evaluated. Based on the results, some discussions are made. The first test results give an idea of how the ESP32 camera works and the special features of the ESP32 camera. We also learn about video quality and how to implement black and white video streaming with an ESP32 camera. The second test result sent by the pulse oximeter and heart-rate sensor shows its accuracy in detecting abnormal readings. The accuracy of the device is shown. The sensor delay time is confirmed. The third test was done to inspect the response of a buzzer after detecting abnormal readings from the pulse oximeter and heart-rate sensor. The fourth test is run through the Blynk web interface, which displays the heart-rate and oxygen values. The test also confirms the operation of the Tasker app, which sends the alert text messages to the guardian’s mobile device when abnormal heart-rate readings are detected. Based on the results of the test, these are the discussions that can be held. The table 5.6 shows the components used in various tests and their results(OK/not OK).

Functionalities		Particular Constraints	Used Technologies	Existing Technologies
Detection of readings	< 100Bpm	Validity > 90%	Pulse-Oximeter	PIR Sensor Temperature Sensor Skin Color Sensor
	> 100Bpm	Validity < 70%		
Monitoring of user		High Validity	ESP-32 Camera	Web Camera CMOS
Surveillance		Coverage of user's surroundings	ESP-32 Camera	Web Camera CMOS
Face Recognition		High Validity > 80%	ESP-32 Camera	Nest Hello Mini OV 7690
Communication (Informing guardian)		High Validity > 90%	Blynk Web Server Tasker Application	Bluetooth GSM
Interface		High Validity > 75%	Blynk Web Server	Webpage with domain hosting for security

Figure 5.6: Table of results

Chapter 6

System Limitations

As we were researching the area of our research topic, we found a lot of suitable devices or sensors to use in our projects. To make our project more accurate to avoid false alarms, we came up with so many ideas. Unfortunately, due to some limitations, we couldn't proceed with that. Moreover, we couldn't buy some products to build our prototype due to lack of permission. Hence, we had to include smartphones as one of the major parts of our project. In this chapter, we discussed the limitations that we faced while working on this project.

- **Raspberry Pi:** For any IoT based project, Raspberry Pi is the best fit due to its capacity of handling multitask. In addition, multiple sensors can be added to it, which is the major part of our project. However, we couldn't use Raspberry Pi for our project as it has been stocked out and very few pieces can be found with a very high price. As we are trying to build a highly cost-effective device for women safety, Raspberry Pi is not the best fit for that. Hence, we decided to use NodeMCU embedded with ESP8266 Microcontroller, which is much more cost-effective than raspberry and could fulfill all the requirements.
- **Voice sensor:** To provide more accurate and efficient results and to avoid false alarms in non-dangerous situations, we wanted to use a voice sensor. So that they can easily initiate the defense mechanism by giving a voice command. Not always it would be possible to press the press button by the victim. In that case, using voice commands would be much easier. Unfortunately, we later found out it would create more false alarms. Outside noises, crowded areas or while having any conversation, the voice sensor would pick up commands and initiate the mechanism. That's why we had to find alternative ways to solve the problem.
- **GPS GSM:** Initially, we decided that we would build a device that detects the danger situation and would send location to the nearest one. To do that, we needed to implement GPS GSM in our device. But unfortunately, we are unable to buy one due to the IMEI number. Only the registered public could buy them to use. Hence, we will have to use the mobile's GPS and GSM for sending immediate location based messages.
- **Delay handling:** As we mentioned earlier, we were willing to use a voice sensor, but it wasn't a good match. That's why we decided to set a delay before initiating the defense mechanism. However, if we did set a delay, the

pulse oximeter and heart rate sensors were showing difficulties reading the vitals. Sensors don't work when we add extra delay for other purposes.

Chapter 7

Conclusion

Furthermore, to conclude, this system reinforces the idea of gender equality by providing a self-defense mechanism for women in the street in a dangerous situation as they are more prone to attacks. Our device is inspired by a real-life scenario faced by women. Considering the fact that a woman can be attacked in multiple ways, we have tried to install a pulse oximeter and heart-rate sensor that measures heart-rate (pulse) and oxygen levels, both of which are very reliable parameters in case of an emergency. We have connected this device to a Blynk web server which displays these user parameters (heart-rate and oxygen values) to the server, from where the parent can access the data. This device also comes with an ESP-32 camera which can stream live video, and also has face detection to identify the attacker. We send text messages and location using the Tasker app. All these features make this device very well-thought-out and realistic to use, and ensures women's safety, which is our main purpose in the research.

Thus, our device can effectively acquire all the goals that we planned initially. Using the manual system adjustment options (start streaming and stop streaming), the guardian can see the stream and stop it according to his/her preference, even if the user is perfectly safe. Below are some points achieved by the system we developed:

- Always monitors the user. This device can monitor the user when she is outdoors via sensors (MAX30101, ESP-32 CAM) installed in the device. The user can also be monitored through the Blynk web interface.
- ESP32 camera is enabled if there is any abnormal condition detected. In order to watch the video streaming, the ESP32 camera must be enabled.
- The sensor also has a delay of 6 seconds, so in case false positives are generated, and the device is turned on, the user can manually turn off the device using a stop button.
- The Blynk web interface is created. The guardian can access user data (heart-beat, oxygen level) via the Blynk web interface.
- Active sensors are continuously present on the field, thus reducing the necessity for human intervention.
- The guardian can track the movements of the user, via video streaming. For notable pulse or oxygen reading, the device will immediately turn on the alarm

and send alert text messages to the guardian. The guardian can take immediate response by turning on the video streaming and tracking her location, and also inform the police.

Chapter 8

Future Scope

The device was integrated based on a real-life scenario faced by women in the streets. However, there are still some improvements to be made in our device. The future scope of our project is briefly described below in the following bullet points:

- In our working model, we used a lithium-ion battery, which can be replaced by a polymer battery to reduce the size of the battery and the device.
- Other means of safety, like PIR sensors or skin detection sensors can be added to the product, to detect alert situations.
- Installing an SOS Light indicator which will be flashing a warning light, thus continuously drawing the attention of the surrounding people that the user is in danger.
- The wearable device can also be made waterproof to prevent short-circuiting.
- Rather than just working on smaller areas, the application must be widened and made much more effective.
- A voice sensor can be added which can be turned on specific keywords like “help”. This feature can be built as a backup, because in a panic situation the automatic reflex of a woman would make her scream or make any form of distress noise which is captured by the voice sensor.
- An electric stun device which would momentarily stun the attacker and allow the user to escape. The electric shock generated would be mild, causing no permanent damage, but disarming the attacker momentarily, thus protecting the user.
- Buying a separate domain hosting and creating a user interface where only authorized people (guardians) can have access to user data, thus ensuring greater security.
- In our working model we used ESP8266 microcontroller embedded with NODEMCU configuration, which can be replaced by Raspberry pi due to its multitasking and fast processing ability, thus making the device more effective in case of an assault. Raspberry Pi is more expensive and stands as a barrier in making a cost-effective device.

- We may use machine learning in our device to improve the performance like automatically avoiding false alarms. The dataset can be analyzed online so that it can improve its performance based on users behavior.

Chapter 9

References

- [1] Hussain, S. M., Nizamuddin, S. A., Asuncion, R., Ramaiah, C., Singh, A. V. (2016, September). Prototype of an intelligent system based on RFID and GPS technologies for women safety. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 387-390). IEEE.
- [2] Viswanath, N., Pakyala, N. V., Muneeswari, G. (2016, May). Smart foot device for women safety. In 2016 IEEE Region 10 Symposium (TENSYMP) (pp. 130-134). IEEE.
- [3] Helen, A., Fathila, M. F., Rijwana, R., Kalaiselvi, V. K. G. (2017, February). A smart watch for women security based on iot concept 'watch me'. In 2017 2nd International Conference on Computing and Communications Technologies (ICCT). IEEE.
- [4] Sapna, Sangeetha, Raghuttam. (2015). Advanced Intelligent Security and Self-Defence System for Human Beings. International Journal of Science and Research (IJSR).
- [5] Khandelwal, T., Khandelwal, M., Pandey, P. S. (2018, October). Women Safety Device Designed using IoT and Machine Learning. In 2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation. IEEE.
- [6] Ruman, M. R., Badhon, J. K., Saha, S. (2019). Safety assistant and harassment prevention for women. In 2019 5th International Conference on Advances in Electrical Engineering (ICAEE). IEEE.
- [7] Seth, D., Chowdhury, A., Ghosh, S. (2018). A Hidden Markov Model and Internet of Things Hybrid Based Smart Women Safety Device. In 2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE). IEEE.
- [8] Jatti, A., Kannan, M., Alisha, R. M., Vijayalakshmi, P., Sinha, S. (2016). Design and development of an IOT based wearable device for the safety and security of

women and girl children. In 2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT). IEEE.

[9] Patel, J., Hasan, R. (2018). Smart bracelets: Towards automating personal safety using wearable smart jewelry. In 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC). IEEE.

[10] Bhardwaj, N., Aggarwal, N. (2014). Design and Development of “Suraksha”- A Women Safety Device. International Journal of Information Computational Technology.

[11] Nikam, Jagtap, Dhumal, Gupta, (2014). Improved Security for the Girls Safety. International Journal of Innovative Research in Advanced Engineering (IJIRAE).

[12] Sogi, Chatterjee, Nethra, Suma. (2018). SMARISA: a raspberry pi based smart ring for women safety using IoT. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA). IEEE.

[13] Ahir, Kapadia, Chauhan, Sanghavi, (2018). The Personal Stun-A Smart Device For Women’s Safety. In 2018 International Conference on Smart City and Emerging Technology (ICSCET). IEEE.

[14] Mala, Pavithra, Swetha, Yashika, Varsha, (2020). A Raspberry Pi Based Smart Wrist Band for Women Safety Using IoT. European Journal of Molecular Clinical Medicine.

[15] Toney, Jabeen, Puneeth, (2015). Design and implementation of safety armband for women and children using ARM7. In 2015 International Conference on Power and Advanced Control Engineering (ICPACE). IEEE.

[16] Bhoopal, Rajasimha, Kavya, Sreevidya, (2019). CHILD SAFETY WEARABLE DEVICE USING WIRELESS TECHNOLOGY.

[17] Warke, Sanmay, Ghodake, Sonawane. SECURITY SYSTEM BY USING STUN DEVICE FOR women’s safety.

[18] Nikam, A., Jagtap, A., Dhumal, M., Gupta, N. (2014). Improved Security for the Girls Safety. International Journal of Innovative Research in Advanced Engineering (IJIRAE).

[19] Dinah, Sivasankari, Venkatesh, Ashokd, Prashanth. (2020). Women’s Safety Security System using Raspberry PI. International Journal of Engineering and Advanced Technology (IJEAT).

[20] Senthamilarasi, Bharathi, Ezhilarasi, Sangavi. (2019). Child Safety Monitoring System Based on IoT. In Journal of Physics: Conference Series. IOP Publishing.

[21] Priyanka, S., Roshini, K. P., Reddy, S. P., Rakesh, K. (2018). Design and

implementation of SALVUS women safety device. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT). IEEE.

[22] Al-Suwaidi, G. B., Zemerly, M. J. (2009). Locating friends and family using mobile phones with global positioning system (GPS). In 2009 IEEE/ACS International Conference on Computer Systems and Applications. IEEE.

[23] Tabu, Suryanarayana. (2020). IoT Based Home Monitoring System. Bachelor Thesis in Electrical Engineering. Dept. of Mathematics and Nature Sciences Blekinge Institute of Technology (Karlskrona, Sweden).

[24] Tartagni, M., Guerrieri, R. (1998). A fingerprint sensor based on the feedback capacitive sensing scheme. IEEE Journal of Solid-State Circuits.

[25] Lee, J. W., Min, D. J., Kim, J., Kim, W. (1999). A 600-dpi capacitive fingerprint sensor chip and image-synthesis technique. IEEE Journal of Solid-State Circuits, 34(4), 469-475.

[26] Moodbidri, A., Shahnasser, H. (2017). Child safety wearable device. In 2017 International Conference on Information Networking (ICOIN) (pp. 438-444). IEEE.

[27] Sinha, Sengupta, Sarkar, Singh, Islam. (2019). Emergency Alert System for Women's Safety. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering.

[28] Shamna, Kavya, Nores, Parvathy, Soniya, Patil. (2019). IoT Based Smart Foot Device For Women Safety. International Journal Of Research In Engineering And Technology(IJRET).

[29] Akshay, Sachin, Prasanna, Chithra. (2020). Women Safety Jacket with Smart Safety Protocol and Screaming Sensor. International Journal of Engineering Research Technology (IJERT).

[30] Sindhu, Subhashini, Gowri, Vimali. (2018). A Women Safety Portable Hidden Camera detector and jammer. International Conference on Communication and Electronics Systems.

[31] Ramachandran, Dhanya, Shalini. (2019). A Survey on Women Safety Device Using IoT. Proceeding of International Conference on Systems Computation Automation and Networking.

[32] Tejonidhi, Aishwarya, Chaitra, Dayana, Nagamma. (2019). IOT Based Smart Security Gadgets for Women's Safety. 1st International Conference on Advances in Information Technology.

[33] M. R. Ruman, J. K. Badhon, S. Saha. Safety Assistant And Harassment Prevention For Women. (2019). 5th International Conference on Advances in Electrical

Engineering (ICAEE),

[34] Samiksha, Karan, Pushkar. Women Security Gadget. (2016, March). International Journal Of Research In Engineering And Technology (IJRET).

[35] Swapnali, Saloni, Sonali, Amol, Bhosale. Electronic Jacket For Women Safety. (May, 2017). International Journal Of Research In Engineering And Technology (IJRET).

[36] Sethi, Juneja, Gupta, Pandey. (2018). Safe Sole Distress Alarm System for Female Security Using IoT. Proceedings of First International Conference on Smart System, Innovations and Computing. Smart Innovation, Systems and Technologies, Vol 79. Springer, Singapore.

[37] Mirjami, Helen, Pekka, Susanna. (2014). Implementation of a Wearable Sensor Vest for the Safety and Well-being of Children. The second international Workshop on Body Area Sensor Networks.

[38] Raganna, Nithesh, Neha, Shrivastav, Musaguppi. (2021). Iot based night patrolling robot for women safety. International Journal of Modern Agriculture.

[39] George, Cherian, Antony, Sebastian, Antony, Rosemary. (2014). An Intelligent Security System for Violence against Women in Public Places. International Journal of Engineering and Advanced Technology (IJEAT).

[40] Arias, Orlando. (2015). Privacy and security in internet of things and wearable devices. IEEE Transactions on Multi-Scale Computing Systems.