

SAFETY BAND WITH NEARBY DEVICE ALERT SYSTEM

By

Vigneswaran Jaganathan (B00122873) MEng (IoT).

A thesis submitted to Technological University Dublin, for the
degree of Master of Engineering in Internet of Things
Technologies.

Supervised by Mr. Benjamin Toland

Department of Engineering

TU Dublin – Blanchardstown Campus, September 2019

ABSTRACT

As per the survey of World Health Organization (WHO) on violence against women they indicate, globally about **1 in 3 (35%)** of women worldwide have either physical or sexual abuse in their lifetime. Harassment can negatively affect women's physical, mental and sexual conditions. Many countries proposed various laws for the welfare of women safety. But still, each year it is being increasing day-by-day due to lack of help for a woman during the emergency situation (Who.int, 2019). The main aim of the proposed research work is to create a wearable Safety Band which sends alert notification to the emergency contact numbers as well as the emergency alert message with real time location will be send to the people within certain distance who uses the same band. These Band users will be filtered out by a filter algorithm and sends the message via Twilio SMS API which runs on the cloud for sending the SMS to the trustee users within victim location. All the above module will be working with the help of Wi-Fi data from the mobile. In case, if the women in emergency where there is no mobile network coverage, they can't send the emergency alert to anyone. So, we have come up with an idea by using the SIGFOX module. SIGFOX has a good coverage all over the EU countries and also being expanded all over the world. So, when the women clicks the button where there is no network coverage, SIGFOX will be activated for passing the real time Geolocation to the people in their emergency contact and nearby people using the same brand band by filtering algorithm.

DECLARATION

I certify that this thesis which I now submit for examination for the award of Master of Engineering in Internet of Things, is entirely my own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my work.

This thesis was prepared according to the regulations for graduate study by research of Technological University Dublin and has not been submitted in whole or in part for another award in any other third level institution.

The work reported on in this thesis conforms to the principles and requirements of TU Dublin's guidelines for ethics in research.

TU Dublin has permission to keep, lend or copy this thesis in whole or in part, on condition that any such use of the material of the thesis be duly acknowledged

Signature: Vigneswaran Jaganathan Date: 08-09-2019

ACKNOWLEDGEMENTS

I would like to extend thanks to the many people, who so generously contributed to the work presented in this thesis.

Special mention goes to my enthusiastic supervisor, Benjamin Toland. My MEng has been an amazing experience and I thank Ben wholeheartedly, not only for his tremendous academic support, but also for giving me so many ideas and knowledge about new technologies.

Similar, profound gratitude goes to Arnulf Horn who has been a truly dedicated mentor for my project. I am particularly thanking Arnie for his constant faith in my research work, especially for his motivation and support.

Finally, I would like to thank my parents for their wise counsel and sympathetic ear. Moreover, I would like to thank Priya, who were of great support in deliberating over our problems and findings. They are the most important people in my world, and I dedicate this thesis to them.

With regards,

Vigneswaran Jaganathan

ABBREVIATIONS LIST

IoT	Internet of Things
WT	Wearable technology
WHO	World Health Organisation
EU FRA	European Union Agency of Fundamental Rights
IDE	integrated development environment
EU	The European Union
SOS	save Our Souls
FOR	Fear of Rape
FOC	Fear of Crime
UNICEF	United Nations International Children's Emergency Fund
AVR	Automatic Voltage Regulator
LoRa	short for Long Range
NB-IoT	Narrowband IoT
BLE	Bluetooth Low Energy
REST	Representational State Transfer
DNS	Data Stream Network
Gmap	Google Map
IaaS	Infrastructure-as-a-Service
KNN	K-Nearest Neighbor
ARM	Advanced RISC Machines
GPRS	General Packet Radio Service
GRS	Galvanic Skin Resistance
HMM	Hidden Markov Model
ML	Machine Learning
Wi-Fi	Wireless Fidelity
AWS	Amazon Web Service
IBM	International Business Machines Corporation
RFID	Radio Frequency IDentification
LAN	Local Area Network

WAN	Wide Area Network
LTE	Long Term Evolution
M2M	Machine 2 Machine
GPIO	General Purpose Input/ Output)
I/O	Input and Output
UUID	Universally Unique IDentifier
SSID	Service Set Identifier
ADC	Analog Digital Communication
SHA	Secure Hash Algorithm
AES	Advance Encryption Standard
DES	Data Encryption Standard
MQTT	Message Queuing Telemetry Transport

Contents

ABSTRACT	I
DECLARATION	II
ACKNOWLEDGEMENTS	III
ABBREVIATIONS LIST	IV
LIST OF FIGURES:	IX
TABLE OF TABLE	X
1. INTRODUCTION	11
1.1 BACKGROUND	11
1.2 PROBLEM STATEMENT	15
1.2 CONTEXT OF STUDY.....	16
1.3 RESEARCH QUESTIONS.....	16
1.4.1 PRIMARY RESEARCH QUESTION.....	16
1.4.2 SECONDARY RESEARCH QUESTION.....	16
1.5 RESEARCH AIM AND OBJECTIVES	17
1.5.1 OBJECTIVE	17
1.5.1 OBJECTIVE 1 – OVERALL BACKGROUND RESEARCH	17
1.5.2 OBJECTIVE 2 – HARDWARE.....	17
1.5.3 OBJECTIVE 3 – BACKEND	17
1.6 RESEARCH IMPACT.....	17
1.7 THESIS OUTLINE.....	18
2 LITRATURE REVIEW	20
2.1 LITERATURE REVIEW INTRODUCTION	20
2.2 EXISTING PRODUCTS AND RELATED WORK	20
2.2.1 VIOLENCE AGAINST WOMEN.....	20
2.2.2 EXISTING WEARABLES DEVICES FOR WOMEN SAFETY	21
2.2.3 EXISTING PRODUCTS:.....	25
3. TECHNOLOGICAL REVIEW	26
3.1 INTERNET OF THINGS.....	26
3.1.1 DEFINITION OF INTERNET OF THINGS:.....	26
3.1.2 IOT CHARACTERISTICS:.....	27
3.1.3 IOT ARCHITECTURE:	28

3.1.4 IOT APPLICATION AND TECHNOLOGIES:	30
3.2 LPWAN	31
3.2.1 SIGFOX	32
3.2.2 LORA	34
3.2.3 NB-IoT	35
3.3 BLUETOOTH:	36
3.4 GEOLOCATION-BASED MOBILE APP DEVELOPMENT	38
3.5 CLOUD PLATFORM	38
3.5.1 AWS	39
3.5.2 IBM WATSON IOT	41
3.5.3 GOOGLE – Firebase	42
3.6 SMS API.....	44
3.7 PYCOM.....	44
4 DESIGN.....	46
4.1 PROPOSED SYSTEM DESIGN.....	46
4.1.1 WORKING MODULE	47
4.1.2 TRIGGER SENDS TO SIGFOX	49
4.2.1 PYCOM FIPY/ EXPANSION BOARD.....	51
4.2.2 SIGFOX.....	53
4.2.3 PYBYTES.....	55
4.2.4 TWILIO SMS API SETUP.....	55
4.2.5 ADD FIREBASE AND ANDROID STUDIO	56
5. IMPLEMENTATION.....	60
5.1 BUTTON CLICK.....	60
5.2 BLUETOOTH.....	61
5.3 MOBILE APPLICATION.....	61
5.3.1 FB Query:.....	63
5.3.2 WEBAPI	65
5.4 SIGFOX.....	65
5.4.1 WEB API	66
6. RESULTS.....	68
6.1 INSTALLING SAFETY BAND MOBILE APPLICATION.....	68
6.2 LIMITATIONS.....	71
7. CONCLUSION	73

7.1 FUTURE WORK.....	73
BIBLIOGRAPHY:	74
APPENDIX A.....	81
APPENDIX B.....	81

LIST OF FIGURES:

- Fig 1: domestic abuse in Ireland
- Fig 2: EU wide, Violence against women in their lifetime
- Fig 3: IoT in 2020
- Fig 4: Architecture of an IoT system design
- Fig 5: Distributed systems in real time IoT
- Fig 6: Sig-fox working
- Fig 7: Lora overview
- Fig 8: Bluetooth node
- Fig 9: Bluetooth low energy
- Fig 10: collection Geo-location data
- Fig 11: AWS IoT
- Fig 12: Cloud Watch working
- Fig 13: IBM watson IoT Architecture
- Fig 14: Working of IBM watson IoT
- Fig 15: Google Firebase
- Fig 16: Traditional vs Firebase
- Fig 17: System Design
- Fig18: Trigger event sends to Mobile Application and Sigfox
- Fig19: Filter flow of Mobile application
- Fig:20 Sigfox Flow
- Fig 21: Twilio Integration
- Fig 22: over all Pycom setup
- Fig 23: Firmware Update
- Fig 24: Creating Sigfox account 1
- Fig 25: Pycom devkit Activation
- Fig 26: Pybytes API credentials
- Fig 27: Twilio SMS API setups
- Fig 28: Firebase and android studio
- Fig 29: adding Firebase in android studio
- Fig 30: Firebase Projects

Fig 31: Firebase dashboard

Fig 32: Firebase Initialize

Fig 33: Firebase web API deployment

Fig 34: Implementation

Fig 35: Bluetooth Implementation

Fig 36: Firebase cloud, Twillio, Android Integeration

Fig 37: Bluetooth Connection Establishing

Fig 38: Filtering Process in Android Back-end

Fig 39: Firebase Database

Fig 40: URL request

Fig 41 Web API for mobile application

Fig 42: Sigfox Callback

Fig 43: Web API for sigfox

Fig 44: Installing Safety Band Mobile application

Fig 45: Location Access Enable

Fig 46: Adding Emergency contact

Fig 47: Display of Emergency Contact

Fig 48: location Updated in Database

Fig 49: Message received to emergency contact

Fig 50: Message received to nearby devices

Fig 51: Location of Victim

Fig 52: Bluetooth advertising to connect with client

Fig 53: Twillo API Credentials

TABLE OF TABLE

Table 1: Domestic violence, Irish women vs rest of the EU women

Table: 2 violence faced in childhood by Irish women and other EU region

Table: 3 SigFox Feature

1. INTRODUCTION

The first chapter of this thesis begins with detailed background research on the evolution of the Internet of Things and wearable technology. Moreover, it also explains the motivation of this research presented in this thesis. Subsequently, the problem statement, research aim, objectives and hypothesis are presented to show the study of this thesis systematically. In the last section of this chapter, an overview of the structure of this thesis is provided.

1.1 BACKGROUND

Recent trends are open to the era of the Internet of Things (IoT). It is one of the emerging technologies in the modern world, which is always being expected by the forthcoming generation (Ghanchi, 2018). In the last five years, there was a big revolution in the world of technology, from phones to cities all are becoming smarter. The market value of wearable technology has grown tremendously over the last few years generation (Ghanchi, 2018). Moreover, smartwatches, health tracker bands are one of the high selling gadgets, with a market value of USD 100 billion by 2018 (Lamey, 2018). Wearable Technology (WT) is one of the emerging technologies in the spot-light, since 2017 nearly 77 million wearable devices were been used by the U.S adults (Crucius, 2018). WT are mainly used for enhancing smart communication, interface with other smart devices and compatibility (Wade 2017).

Around the world, sexual abuse and rape are increasing every day, thousands of women and girls are being affected. However, there are many laws for rape punishment, but still, the numbers are increasing every day. Every country has different types of laws, for example, in Saudi Arabia punishments like hanging, stoning, lashing and beheading are given for crimes such as murder, rape and robbery. Moreover, according to statistics, 0.3 rapes per 100,000 population occurs in Saudi (Straits, 2018). India's official crime data shows the number of reported violations of children increased from 8,541 in 2012 to 19,765 in 2016 (Binick, 2019). According to the recent report from Amnesty International, violence against women in Ireland is less compared to other countries in EU but still in some women are affected, the report says, women affected in violence have both mental and physical pressure (Condon, 2019). According to the Sexual Abuse and Violence in Ireland (SAVI) report (2002) found 1 in 4 women had experienced in sexual/ mental harassments in their lifetime. From January 1996 to June 2005, nearly 109

women were killed in Ireland. Almost half were by the women's partner or ex-partner. On the other hand, a study by Women's Aid in the 1990s found that 1 in 5 women who had experienced in violence/ rape in Ireland never reports the Garda.

Survey According to FRA

European Union Agency for Fundamental Rights (FRA) presented a survey on 05/03/2019 on violence against women in the EU. The purpose behind this survey was to produce dependable, steady and first-hand data to analyze them on the experiences of violence they faced (Fra.europa.eu, 2014). The sample was collected by face to face interview methodology with 42,000 random women aged 18-74 years across the whole of the EU, which gives an average of 1,500 women in each country. The interview consisted questionnaire asking experiences of physical, sexual and psychological violence which included stalking, sexual harassment, the experience of the violence by their partners, also known as domestic violence. Below is the data of the survey comparing the average abuse faced by Irish women in their life-time. The Irish women faced lesser sexual violence compared to the women in rest of EU from their partner or non – partner since the age of 15 i.e., 8% of Irish women compared to 11 % women in rest of EU.

The following comprises the data on Irish women compared to women in the rest of the EU region facing various types of domestic violence by a partner.

TYPE	IRISH WOMEN (%)	REST OF EU WOMEN (%)
Psychological violence	31	43
Controlling behavior	23	35
Economic violence	10	12
Abusive behavior	24	32

Table 1: Domestic violence, Irish women vs rest of the EU women

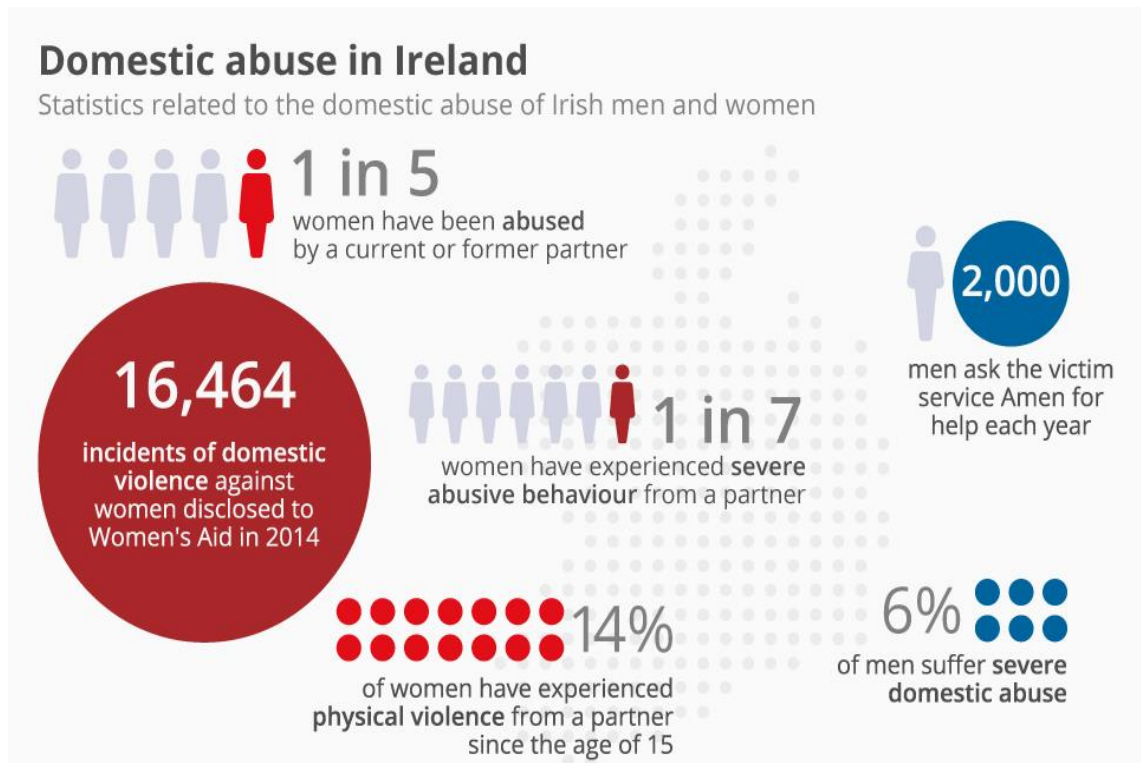


Fig 1: domestic abuse in Ireland

This data shows that Irish women have faced less violence than women in the rest of the EU region. Also, Irish women contacted the police for help more compared to women in the rest of the EU region, 21% to 14% by a partner and 16% to 13% by a non-partner. 26% of women in Ireland faced physical or sexual abuse before the age of 15 to 33% of average women in the EU region (Cosc.ie, 2019).

The table below shows observation of categories on violence faced in childhood by Irish and rest of EU region women.

CATEGORY	IRISH WOMEN (%)	EU REGION WOMEN (%)
Father, step/foster father	23	58
Male doctors, priest and teachers	13	6
Female acquaintances, friends or neighbors	17	4

Table: 2 violence faced in childhood by Irish women and other EU region

- More women in Ireland are prone to violence than in rest of EU (33% to 27%).
- More women in Ireland report if they find anybody in their family or friends circle being a victim of domestic abuse, 41% Irish women to 39% women in rest of EU region.
- Only 42% women in Ireland compared to 49% women in rest of EU region are known to laws and political initiatives to counter domestic violence against them (Cosc.ie, 2019).
- According to the survey carried out in the whole of EU (28 member states) according to FRA main results. Almost 5% i.e., 9 million women have faced stalking last year. 1 in every 5 women have been stalked over for 2 years. Because of some serious case of stalking 23% women changed their email, address and phone numbers. In EU 55% have been sexually harassed. Boss, colleagues or customers were the biggest predators for 32% of victims. The average of women in top management and qualified professions have faced sexual harassment is 75%. Cyber sexual harassment have been faced by 20% women aged 18-29 (Cosc.ie, 2019).

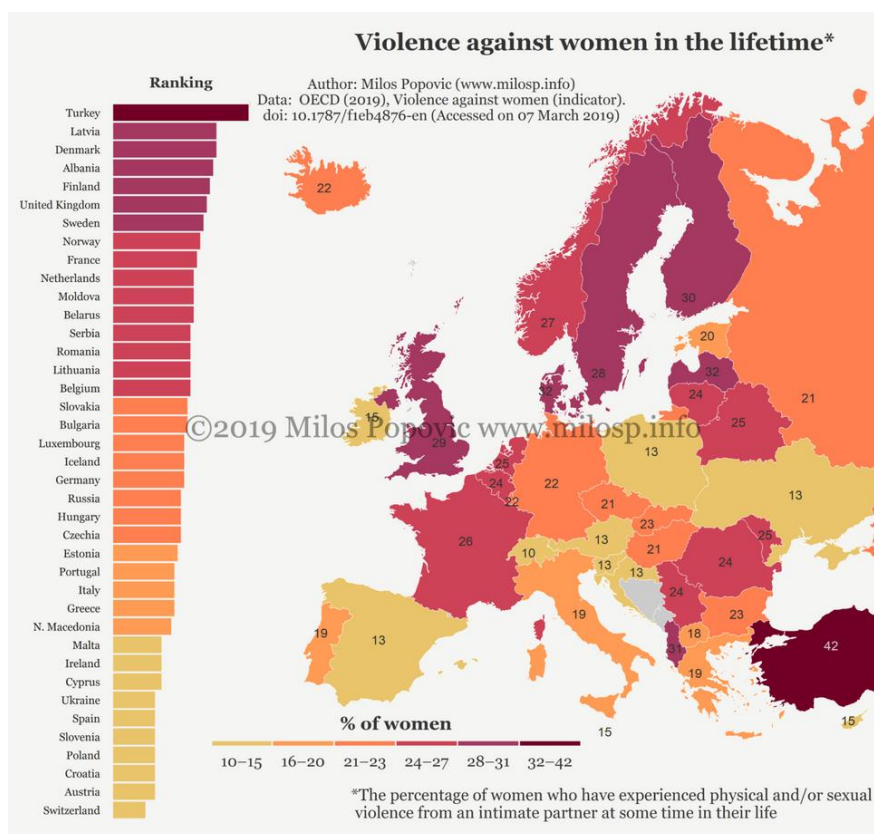


Fig 2: EU wide, Violence against women in their lifetime

1.2 PROBLEM STATEMENT

In recent years, violence against women's is increasing day-by-day at an increasing rate. According to FRA- European Union Agency for Fundamental Rights, a survey was carried out on "Violence against women: an EU-wide survey". In the 28 European Union Member States, 1 in 3 women has experienced physical or sexual violence (at least once since she was 15) 8% of women in the last 12 months. Moreover, 11% of women have experienced some form of sexual violence, and 5% of women have been raped (1 in 5 women had been sexually harassed in the last 12 months). Nowadays, women's are being excelled in all the working fields, however, it is now becoming an exigency for them to travel late night from their firm or to visit some isolated locations as a part of their office work, during this time when they are all alone in late nights many violence or harassments occurs (Fra.europa.eu, 2014). However, it is also very important to highlight the Fear of Rape (FOR) and Fear of Crime (FOC) among the women in the modern society. A study conducted at the University of Queensland during 1992 on "Understanding Women's Rape Experiences and Fears", examined both psychological elements of FOR and women's experience in physical/ Sexual harassment. According to the study, Samples were taken randomly under each age group from 15 to 70, victims were questioned based on their rape experience in their lifetime as well as their Mental/ physical condition after this incident (O'donovan 2007). The findings concluded with the mixed review, such as 10% of women's were not fearful as they know they can handle the situation, and 50% are slightly fearful of being raped. However, one-quarter of women are extremely dread in that situation and also got afraid of being killed (O'donovan 2007). UNICEF on the International day suggested few ways to handle the emergency situation. One of the main suggestions that was highlighted by the speaker, is to have some smart devices to alert the nearby Garda stations or family members during the emergency situation. As technology grows, there are many smart devices that are in the market for women's (Alleman et al., 2018).

Even though the world has been developed so much in technology, still many people are unaware of it or lack of knowledge in using it. During the emergency situation, everyone uses their phone to indicate their close mates for help. There may be many external factors that affect during phone communication like Network coverage. All these factors have been taken as parameters of the problem statement. At the same time, if the women had

any other device other than a mobile phone to indicate the emergency situation it would be so easy for them to send SOS alert to the family members, friends or near Police station. In the previous existing products and application, they have few drawbacks and problems during real-time implementation. The main problems that are in the existing devices are that all the products use a GSM module to transmit the location of any data to the mobile phone. Importantly, to send SMS through GSM module network coverage is mandatory. When the women got stuck in an isolated place where there is no network coverage, she cannot alert the emergency situation to the family or the friends. At the same time, one more problem is that if the women are far away from their home and when they need help in an emergency case her family/ friends can't reach in the short time. So, if there is any technology that has the option to indicate the nearby devices or some other people within a certain radius, they could come and help them in that situation before Garda/ family members reach that place.

1.2 CONTEXT OF STUDY

Numerous studies and survey have been completed on the women safety and the smart application/ devices used for alerting the emergency situation. In a systematic literature survey Nandhini et al. (2018) compared more than 25 papers and proposed systems dealing with different types of wearable devices and application that has been proposed in order to safe guard women's during the emergency circumstances. The majority of proposed system has both merits and demerits. Moreover, all the existing products or the proposed system uses GSM to send the alert SMS to the emergency contacts. This study will look at the specific factors like near device alert and to send the alert SOS SMS to the emergency contacts even though if there is no network.

1.3 RESEARCH QUESTIONS

1.4.1 PRIMARY RESEARCH QUESTION

How does a safety band send an emergency alert to the nearest safety bands (neighbour devices) available?

1.4.2 SECONDARY RESEARCH QUESTION

Can the device loop back to emergency module when there is no network?

1.5 RESEARCH AIM AND OBJECTIVES

The main aim of this thesis is to design and develop a smart wearable wristband for women to indicate the emergency situation (SOS alert) to their pre-stored emergency contact and the nearest devices available around them within certain radius around them.

1.5.1 OBJECTIVE

To solve the research question, a step-by-step procedure has been carried out. Moreover, the whole project has been broken down into small modules to reach the research aim.

1.5.1 OBJECTIVE 1 – OVERALL BACKGROUND RESEARCH

- To deeply understand the core problem and background survey.
- Review existing literature to get better idea on the existing products or proposed system.
- To identify the technologies that will be used for implementation.

1.5.2 OBJECTIVE 2 – HARDWARE

- To deeply understand about Pycom Fipy/ Pytrack and its working.
- To setup the hardware and install required firmware update with required tools.
- Identify an IDE (ATOM) for uploading and editing the code.

1.5.3 OBJECTIVE 3 – BACKEND

Design and develop a mobile application.

- How real time data location stored in Firebase Database
- Build a filtering algorithm (filter nearby devices)
- To identify how SMS API will be triggered.
- To evaluate how fall-back (Sig-fox) module will be activated.

1.6 RESEARCH IMPACT

This research was mainly conducted to enhance Women safety. Many proposed system mostly focused on tracking the current location of the victim and sending SOS alert to the family members or nearby Garda station. Moreover, as the IoT technology has been developed, new development boards and low power communication protocol has been

discovered every year like Sigfox, LoRa, and Many more. However, there is no proper research or a literature on how all these communication protocol will pass the sensor or other data from hardware if there is no network. How will the women alert the emergency situation when she got struck in some isolated location where there is no network?

On the other hand, Researchers have proposed many model to send the SOS alert to the victim's family through GSM module, but if they are far away from home it is not possible to get help from the family members or friends to rescue them. If this product has been launched, it will be very useful for all women in different age group. It will really be helpful to them to go without fear anywhere, even in case if there is any emergency or any bad situation they will get help easily from their close ones and also the people who use the devices will get alert notification that someone needs help, this will have very big impact among the women.

1.7 THESIS OUTLINE

The outline of the Thesis is as given below.

Chapter 2 (Literature Review) discuss the existing products/ literature related to Women Safety / Wearable technologies, Internet of Things. On the other hand, previous works are also compared against this project, and the technologies used by them. Under the

Chapter 3 (Technological Review) discuss detail about IoT and its architecture. Mainly the discussion about the previous existing technology used in the paper and also explains about the technology that will be used in this project. Sigfox, Firebase and Twilio SMS API.

Chapter 4 (Design and Setup) discuss the, overall outline of the project and also individual module design methodology. The setup of the required hardware/ software were explained.

Chapter 5 (Implementation) discuss about the full working method and how the individual objectives are been achieved. Moreover, all the phases of the project working is been

covered like button click, Bluetooth connection, Trigger to Mobile application, Sigfox module.

Chapter 6 (Results) discuss the outcome of the project. Mobile application screenshots and the overall working process. In addition to it, main limitations are explained, difficulties faced during the implementation.

Chapter 7 (Conclusion) discuss the achieved research objective and question and also says about the future work that will be done.

2 LITRATURE REVIEW

2.1 LITERATURE REVIEW INTRODUCTION

In this chapter, research has been done in multiple technologies to form a clear basement, to develop a proper proposed system design. Firstly, to have a better understanding of the core problem, some surveys and case studies were being deeply researched on various perspective. Existing Literature review and previously proposed system analyzed and examined to find the problem in the existing system. However, reviewing the existing products available clearly, differentiate the merits and demerits. Lastly, the technology and techniques that are providing solutions to the existing problem and proposed systems were discussed.

2.2 EXISTING PRODUCTS AND RELATED WORK

2.2.1 VIOLENCE AGAINST WOMEN

Physical/ Sexual harassment and other forms of violence in public places are a day-to-day occurrence for women and girls all around the world. Moreover, it not only occurs in public places but also happens on streets during late night, schools/ colleges, and workplaces. (UN Women 2019). Randall and Haskell (1995) took a survey on sexual violence in women's lives, a group of 420 women living in Canada's capital, Toronto were selected randomly for these face-to-face interviews. All the questions were based on the common problem and effects of various form of sexual abuse/ violence in their lifetime, the problems faced from their childhood (including incest), sexual assault and harassments also documented as many women faced these issues during their childhood. From their findings, they conclude that the male physically assaulted 1 in 4 women in the sample. Intimate, 1 in 2 women experiencing an attempt of being raped. The worst statements were nearly half of the victims experiencing some sexual abuse before reaching 16 years of age. A study was conducted (Koss et al., 1996) in the memory pattern of physically abused women, results proved that after the incident, the victim's memory was affected badly. The author concludes by saying that the physical symptoms and mental pressure are very high after this incident and it takes very long time for them to recover. This study by Brad Ford (2000) says that women who had abused when they are under 15 have lost their focus on their future and went to the depression state. The study

conducted by Sochtinh (2004), leaning self-defence technique most of the North America Universities gave priority in this prevention program for girls

2.2.2 EXISTING WEARABLES DEVICES FOR WOMEN SAFETY

Daniel et al. (2016) suggested in the paper “AVR Microcontroller Based Wearable Jacket for Women Safety” that proposed model is embedded with the sensors to monitor the motion of the user in the wearable jacket. Once the person is in an emergency if they push the emergency button inbuilt GPS module will send an alert notification with the latitude, longitude coordinates of the user. So that they get to know the exact location of that victim

(Viswanath, Pakyala and Muneeswari 2016) Developed a smart foot device using Bluetooth and machine learning. The device will get triggered if the user taps their foot for four times. Once this device is triggered, an alert will be sent to the user mobile via Bluetooth low energy by taking the GPS coordinates of victim an alert will be sent to their family and nearby police station. Moreover, they have analysed the prototype performance like walking and tapping phrase in the machine learning algorithm named as naïve Bayes, which comes under supervised machine learning. So, the machine can differentiate the difference, and when to send the alert. In performance testing, they achieved 97.5 per cent accuracy.

((Saikumar, Bharadwaja, and Jabez 2019) developed android and Bluetooth low energy device based safety system. The device integrated with Arduino Nano controller, Bluetooth module with GPS, GSM and Taser. By considering women safety, they constructed a convenient wearable for the women. This device helps to connect with other electronic devices using Bluetooth low energy. GSM for sending the messages, GPRS for satellite location of the victim during the adverse situation. Finally, Taser is a weapon for the women safety which provides electric shock by this the attack may inactivate temporarily.

Rachan et al., (2018) proposed in the paper “Smart Shield for Women Safety” wearable devices that send an alert notification with their current location through GSM to the pre-registered mobile numbers. Moreover, once the device has triggered, a buzzer will be turned ON as well as live video streaming will be transmitted to pre-registered numbers.

Navya et al (2018) investigated SMARISA: A Raspberry Pi based Smart Ring for Women Safety Using IoT in this paper they use the raspberry pi boards, raspberry pi camera, and button for the implementation of the smart ring. In case of emergency victim need to click

the button once the button is clicked the ring will capture the image of the attacker and send the current image and location of the victim to the emergency contact numbers and police. Additionally, the alarm module is embedded in this ring once the button is pressed the high-frequency alarm is triggered to grab the attention of the people towards the victim.

Richard D Haney (2013) concluded in the paper “Location Sharing and Tracking Using Mobile Phones or Other Wireless Devices”. In this paper, they have used two application named Buddy watch and talk control. Firstly, the buddy watch application communicates with cell phones and other wireless devices which operated with the set of users individually secondly the location with the track has been shared using the cell phone of the buddies in the group.

Hossain et al. (2016) concluded in the paper “Cloud-assisted Industrial Internet of Things (IIoT) – an Enabled framework for health monitoring” the researcher used the IoT internet of things interconnected with the sensors. They stored all the data to the cloud that has been taken from the wearable the researcher used a mobile device. The main disadvantage of this paper is the data has been stored but, they did not use the data anywhere they just stored the massive data from the sensor (wearable) to cloud platform, and it can be connected to the mobile application.

Konstantin et al. (2016) concluded in the paper “Multihop Data Transfer Service for Bluetooth Low Energy” that Bluetooth Low Energy (BLE) is a most efficient protocol that enables good energy-efficient, short-range radio communication. This is used because it consumes low energy/ battery and it will last for many years. The Multihop data transfer for BLE is implemented to reduce the network traffic in IPV6. Nowadays, as technologies are growing massively, many devices have been connected to the internet. At the same time, we need them to connect in a network for data transfer. From this paper, we can have a clear vision of how a Multihop data transfer in BLE network works.

Rajeev et al. (2013) implemented in the paper “Towards the Internet of Things (IoT's): Integration of Wireless Sensor Network to Cloud Services for Data Collection and Sharing” a flexible architecture for incorporating wireless sensor network with the cloud. For this architecture, they used REST-based web service for remote monitoring such as e-healthcare services, smart home etc. This paper clearly explains how the wireless sensor

network transfers data via cloud tool using REST-based Web services as an application layer which can be directly incorporated into other application.

Sandra et al. (2011) say in the paper “Smart Alert Charms for Wireless Devices” a wireless communication device and a method of operating the wireless devices to provide an alert to the devices. The core concept of this paper is to generate a smart alert. This will undergo some basic alert rules or the predefined events and based on that this smart alert charm will create the alert. Moreover, the major advantages are it will take multi inputs and compare the situation, because sometimes false trigger may be generated. So, based on the conditions or rules applies to the events this will be done for women safety alert wireless devices.

(Enefiok and Uzochukwu, 2016) Built an android-based Security and tracking system for school children's, in this application, the parents can fix the destination address, an SOS alert will send if the kid is not going to the destination address. Moreover, when the child is in a home, they can fix a certain radius in the tracking system, if they exceed from that radius an alert will send to the parents mobile with their real-time location.

(Prashanth, Patel & Bharathi, 2017) developed a mobile-based women safety application for real-time database and data-stream network. Initially, Emergency contact numbers need to register in the application. The phone number can be updated and modified; all the data will be stored in the Firebase database. When the user clicks the SOS button, the live location will be sent to the contact numbers they have stored. On the other hand, the mobile application will retrieve the live GPS coordinates, which will be plotted on Gmap with the help of PubNub API. PubNub is a Data Stream Network (DSN) and real-time Infrastructure-as-a-service (IaaS). PubNub API provides many features like to connect and manage the real-time location of the IoT devices and plot their track. The emergency contact numbers can log in into the portal and can see the real-time path where the person is travelling so, this application may be useful for the safety of women.

(Tripti et al., 2019) proposed a paper on Safety Android App which will be connected to a hardware switch. When the button is clicked, a trigger will be generated and sends to the mobile application via Bluetooth. Similarly, (Dharanika & Brindha, 2018) developed a mobile application which will be triggered when the button is clicked thrice. Moreover, the unique feature in this mobile application is sending an alert notification through the K-Nearest neighbour (KNN) algorithm. The same mobile app users will get an instant

notification if they are near within a few radius. However, the GPS based mobile app will be using the Google Maps API. All the user details will be stored in the database. K-Nearest Neighbour (KNN), is one of the most commonly used machine learning algorithms for predicting the closely related data points (Shaw, 2019).

(Priya et al., 2019) investigated on One Touch Alarm for Women's Safety Using Arduino. In this paper, they used the device named as ARM controller for tracking the location of the women they also integrate the emergency button to trigger the action. Once the button is pressed, it starts to trigger the alarm to alert the nearby people and also send the location and emergency message to the contact saved in the emergency column. The device used GSM for sending the messages, GPRS for satellite location with current date and time, Touch sensor for action, Buzzer for alert the nearby people all the devices are incorporated with the Arduino Uno.

(Edward, Vijayakumar & Bhubaneswar, 2018) examined GSM Based Women's Safety Device using Arduino. by this system, the SMS will send with the latitude and longitude of the victim. In this paper, they built the device using Arduino Uno microcontroller and GSM technology for satellite communication which helps to transfer the exact location of the victim. Additionally, they integrated the microphone for the call section and recording facility. In case, if the person is in an emergency, this Arduino device will send the location to the emergency contacts saved. Additionally, it starts the audio recorder of the surrounding. Additionally, it also connects the call mode to the emergency contact when the trigger button is pressed. WEAR is a one-click smart women safety wearable button (Geev 2015), the proposed system is designed in the way that when the button is clicked, it will trigger the SMS alert with the real-time GPS location of the victim.

(A.Jatti et al., 2016) design and developed a wearable device for women and girl children, using the galvanic skin resistance (GRS) and body temperature sensor. This sensor will be triggered based on the sweat glands in the skin. This will be measured when there is a sudden rise in body temperature or physiological arousal (A.Jatti et al., 2016) and the nervous system will be aroused that activated the sweat gland. So, based on this condition, the system triggers an event.

(D.Seth et al., 2018) Highlighted about Hidden Markov Model (HMM) a Machine learning (ML) algorithm, which provides has a deep understanding and predict the insecurities situation based on the minimal trained data. The HMM-IoT senses the sudden

unusual behaviour from the users and activates the alerts request to the emergency contact numbers and nearest police stations. (Nandhini, Moorthi 2018) took a survey various existing Wearable Devices, each and every paper has different event trigger module such as button, Scream, Motion sensor, etc., all these has both pros and cons while triggering an event.

2.2.3 EXISTING PRODUCTS:

Many companies or developers had a similar idea and motto which have come up with many innovative products. Here a few products have been as follows,

A SAFETY PIN: This is a mobile application which is designed for women safety. User has to enable their phone GPS location and can add basic emergency numbers in it. The app also pins the unsafe areas on the map, which will be displayed in the application. So, when the women travel through this location, they will get an instant notification at the same time the emergency numbers will also get the real-time location of them.

HIMMAT: Initially, the user has to register their mobile number with the Delhi Police website for activation. In case of emergency, when the women send SOS alert from the app, live video streaming will be transferred to the Police control room.

SMART BELT: It resembles a normal belt which has a microcontroller (Arduino), screaming alarm and pressure sensor. When the pressure sensor is greater than the threshold, then the device will be activated and notify automatically. The drawback of this product is that the services and actions have been triggered autonomously, which will leave to an emergency at the wrong time.

SHAKE2SAFETY: An easy notify the mobile application if the person is in an emergency the user just need to shake the mobile phone or the power button on the mobile can be pressed four times for sending the SOS alert to the contact number they have stored. Moreover, there is also an option to cancel the false notification in the mobile application

AMULYTE: This Amulyte product is like a necklace which we can be very easy to wear. It has an emergency alert button to send alerts to the contacts added to it with the location (GPS) and Wi-Fi in it. The drawbacks are lacking additional sensors, and if the device is lost, it can't be detected or found so, and someone can miss use it.

3. TECHNOLOGICAL REVIEW

3.1 INTERNET OF THINGS

3.1.1 DEFINITION OF INTERNET OF THINGS:

All electronic device and computational device are becoming smarter and more intellectual day by day. They have been interconnected via internet for communication and transfer or process the data from one place to another place. Especially in the last few years, the Internet of Things (IoT) has tremendous growth. Moreover, it makes people work smarter and also easier. Using internet, the devices can be connected with one another for exchanging information and communication in both wireless and wired technique. IoT act as a kind of network for various application, physical devices, sensors, mobiles, and many other smart objects can be connected using IoT for establishing communication between the objects and collecting information on about everything. Many companies are also trying to enhance the connection of Billions of devices. In 2020 the estimated devices connected will be around 50 billion (Jinesh Ahamed, Amala V. Rajan 2016). By 2020 there will be 4 billion people using IoT, 4 trillion business opportunity will be available, more than 25 million apps will be acting as the middleware for operating the IoT device via smartphone, and 25 billion devices will be connected through the internet, and the devices will produce 50 trillion GBs of data. In addition to this, many countries have started a project called a smart city, where many things will be automated all over the world. One of the main countries is Ireland, for instance: Ireland's Croke Park stadium is one of the biggest stadiums in Europe. Moreover, the project has been collaborated between GAA, DCU, Intel and Microsoft for building the first Full implemented IoT stadium. In 1999, a member of the community of Radio Frequency Identification (RFID) development had invented the IoT idea after a few years. The IoT showing rapid development all over the world. IoT contains three groupings, people to people, machine to machine and people to machine. In addition to this, the M2M machine to machine group is considered to be future of IoT. Using the internet of things, the device can identify their self by intelligence with this, the device can easily access information by other devices and communicate individually. (Keyur K Patel and Sunil M Patel 2016).



Fig 3: IoT in 2020

3.1.2 IOT CHARACTERISTICS:

There are six significant characteristics of IoT, such as safety, connectivity, dynamic changes, interconnectivity, heterogeneity, and Massive scales.

Safety:

The security is one of the mandatory things in accessing the information. Additionally, the taken data may also contain confidential information the data exchanges takes place on the internet, so the security is one of the standards in IoT.

Interconnectivity: IoT is an interconnection of physical objects with accessing and exchanging information. In the IoT, network Interaction takes place between the devices using internet connectivity.

Dynamic changes: The dynamic changes are defined as the state variation of the device for example, location, speed, connection, disconnection and many other things related to the device may vary this condition is defined as Dynamic change.

Heterogeneity: The IoT device, hardware platform and network may be constant or inconstant. The IoT devices may communicate with other network or a hardware platform if the existing one is inconstant.

Massive scales: In the single internet connectivity number of devices can able to connect with each other for transfer information so, the connectivity can manage the larger capacity of sharing devices.

3.1.3 IOT ARCHITECTURE:

IoT architecture consists of four different layers with various technologies to enhance communication between the IoT devices with high performance even though if the user inclined in the network. Additionally, it also helps the application to form a group of components by linking and combine the entire system (Keyur K Patel and Sunil M Patel 2016).

The four Layers are sensor layer, gateway and network, management service layer, the application layer.

- **Sensor layer:**

The sensor layer is also called a device layer which is integrated with sensors the lower layer of the IoT architecture. The physical device which connected with various sensors for collecting data like temperature, speed, humidity, pressure, and much other real-time information. The gathered data can also be converted into various formats like signals of Analog and digital. On top of this, the gateway is needed for many sensors to communicate. The gateway can be enhanced by both LAN and WAN depends on the sensor types. LAN consist of Wi-Fi, ZigBee, Bluetooth and ultra-wideband besides, WAN involve GSM, LTE and GPRS.

- **Gateway and Networks**

The high performance is needed from the tiny sensors for enormous data collection and communication between the devices some devices can interact between the devices without any support medium is called Machine to Machine (M2M). The gateway may be a microprocessor or microcontroller. To establish communication, multiple networks are needed the network may private, public or hybrid networks with various technologies and protocols so, the gateway networks are Wi-Fi, GSM and many other networks are also included.

- **Management service layer:**

Connection and communication of devices are takes places in this service layer. Collection of massive amounts of data from the small sensor may in different formats like signals, events and text data such as location, temperature, and some other events. In the management service layer, the support engine triggers the

communication between the IoT devices. For quick data collection, different tools are used in the IoT systems, for instance, instead of storing a large amount of data in the disks. The analytics tool stored in the random-access memory (RAM) which reduce time and increase the processing speed. In this service, layer information is managed, integrated and controlled. The data filtering and security are also one of the crucial things which take place in the service layer. The filtering is for extraction and providing the quality of data in the management system finally, to provide the data from the hacking and security issues.

- **Application layer:**
This layer consists of application which is an upper layer in IoT architecture which interface between the network and end devices. The application layer consists of a user interaction device (Keyur K Patel and Sunil M Patel 2016).

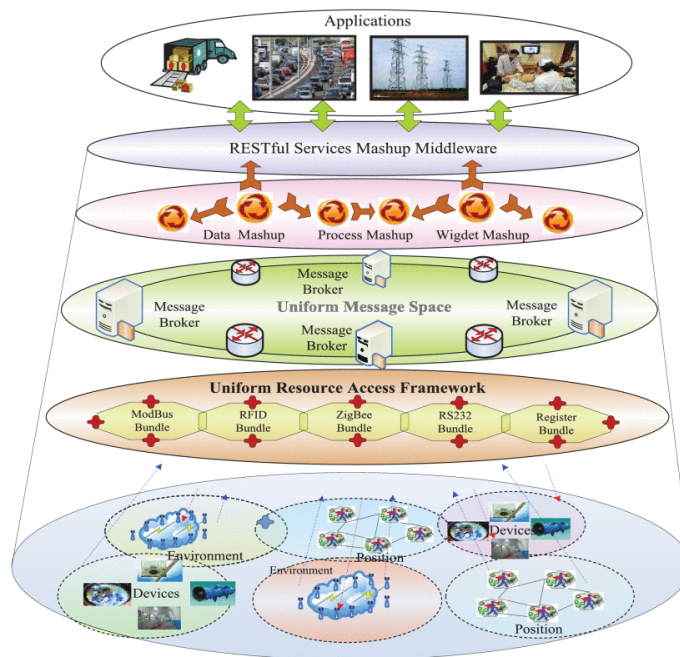


Fig 4: Architecture of an IoT system design

3.1.4 IOT APPLICATION AND TECHNOLOGIES:

(Jinesh Ahamed, Amala and V. Rajan 2016) Nowadays IoT applications are growing wide range in all over the world. IoT application like wearable, smart Homes, smart cities, smart transportation, smart health care system, a lot of applications is enabled with IoT. On top of this IoT enabled applications are very smart, which helps to reduce the human work and helps to decrease the flaws for the IoT application the cloud technologies. For example, smart homes are a popular IoT application with internet facility which mainly for providing the owner for a better quality of life. In addition to this, the wearable is one of the significant IoT application where the user can monitor, control and gather all the information like education, entertainment, medicine and few more data by the wearable gadget which also has the security. The smart city is also one of the major IoT application, which provides a lot of facility for the citizen in terms of environmental quality with low cost and less complexity.

Rajeev et al. (2013) implemented in the paper “Towards the Internet of Things (IoT's): Integration of Wireless Sensor Network to Cloud Services for Data Collection and Sharing” a flexible architecture for incorporating wireless sensor network with the cloud. For this architecture, they used REST-based web service for remote monitoring such as e-healthcare services, smart home etc. This paper clearly explains how the wireless sensor network transfers data via cloud tool using REST-based Web services as an application layer which can be directly incorporated into other application.

All the IoT based device are be somehow connected to a web service where the request-respond of the data or information will be transferred. As the diagram shown below the sensor nodes have been distributed in many different places in the world. The data that has been collected will be passing through the smart gateway where the basic filtering and aggregation is being done. After that is being passed to the distributed server, it starts to monitor the exact problem going on the application. On the other hand, the event-driven the process gets triggered to solve the issue by sending the real-time problem to the analyser to troubleshoot the problem in it.

This can be used by the automobile industry to track their car problem in one place and indicate to the customer about the problem in the car parts and show then the nearest agent where the part can be replaced. Moreover, before the customer reaching there, he will get

an indication that the customer has a problem in his car and the status of the car. So, he can make ready all the required things before the customer comes. It is one of the examples, it can be implemented in each and every field to make the world more advance in technology.

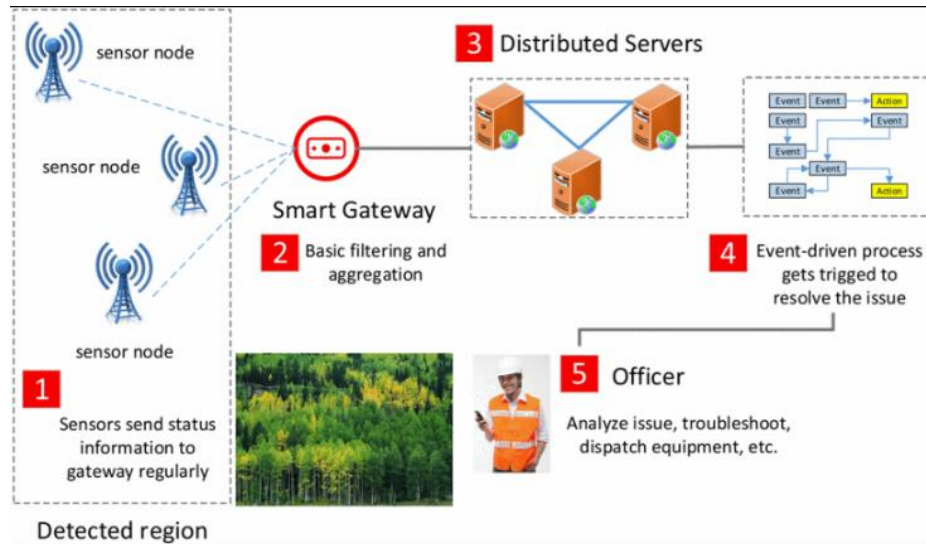


Fig 5: Distributed systems in real time IoT

3.2 LPWAN

Low Power Wide Area Networks (LPWAN) has become a famous and widely used low-rate long-range radio communication technology. For large-scale IoT development and data transfer SIGFOX, LoRa and NB-IoT use LPWAN technology (Kais). Day-by-day IoT technologies have tremendous growth in all major fields. All IoT applications require long-range, low data rate and good battery consumption because when transferring data to long-range more power will be consumed but in short-range radio technologies like Bluetooth, ZigBee takes less energy. To bring the same efficiency in Long-range a new wireless communication technology: Low Power Wide Area Network (LPWAN) has been discovered.

3.2.1 SIGFOX

SIGFOX, a French company that provides low-power wireless communication protocol between IoT devices. Using low power connectivity SIGFOX covers a wide area to transmit or communicate between devices that are been connected in the network so, it is also called as Low power wide area network (LPWAN). Using SIGFOX the data can be transmitted to SIGFOX base station from the base station all the data will be send to the SIGFOX cloud. Moreover, the data that has been transmitted from sensor will be stored in the SIGFOX backend with time stamp and location (SIGFOX device). Based on the client application the SIGFOX impulse information to a lot of users. Using SIGFOX network many real time applications like healthcare, security, and home appliances has been developed. SIGFOX coverage is about 1-3 million square kilometres / population of 240 million people and has maximum coverage of 50 km. Furthermore, SIGFOX provide good data quality and rapid performance over huge distance. (Thomas Michalski 2017). Table 1 shows the main features of SIGFOX.

SIGFOX features

Feature	Value
Frequency	ISM 868 MHz (Europe) ISM 902 MHz (EEUU)ISM 90
Modulation	Ultra-narrow band Power Uplink: DBPSK Downlink: GFSK
Consumption	TX: 51 mA RX: 16 mA
TX power	24 dBm
Messages	140 messages of 12 bytes per day
Price of license	From 1\$ per year and device

Table: 3 Sig-Fox Feature

SIGFOX Working Overview:

Basically, antennas will be fixed on towers in multiple region with certain radius (Europe has a narrower band around 868 MHz).The SIGFOX consist of three division and three

procedure (thomas michaslki 2017). The division involve object, base station and back-end cloud. Firstly, the object is a device of users, which connected to the internet with the help of SIGFOX network. Secondly, base station is a gateway which also an intermediate platform for the users and the network which relate with both the side. Finally, the cloud can also denote as SIGFOX network which contain three process Ultra narrowband (UNB) technology, Differential Phase Shift Keying (DPSK) and Frequency Shift Keying (FSK).

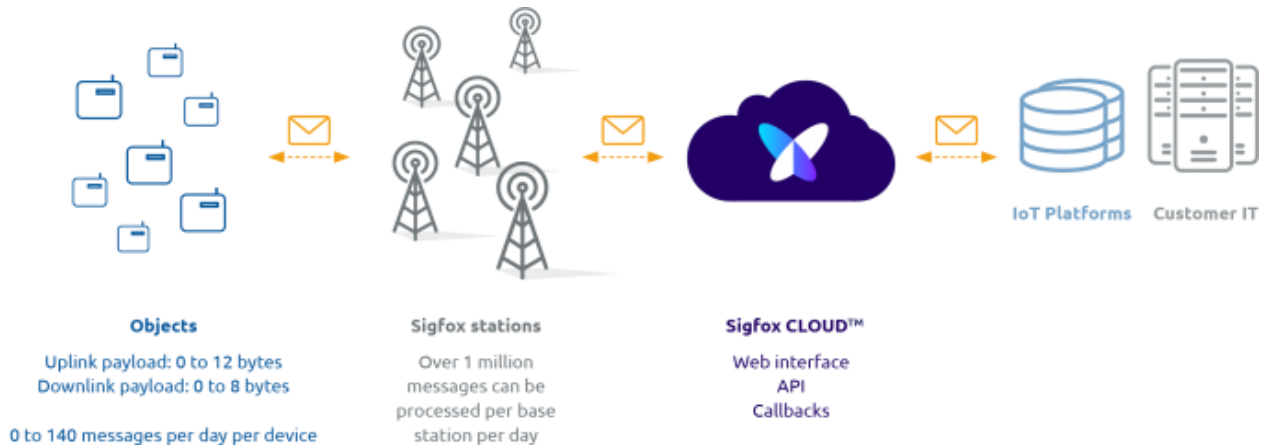


Fig 6: Sig-fox working

Ultra-narrow band (UNB) technology

Less energy Ultra narrowband (UNB) technology consist of infrequent signals 192 KHz which sends limited number of uplink messages per day with 10 minutes time limit here, it can send 140 messages only. And the downlink consists of 4 messages a day uplink messages contain 12 bytes per messages likewise downlink contain 8 bytes per message. Each message is 100 Hz wide and transfer rate of 100- or 600-bits p/s depends on the external factors.

FSK and DPSK

The gateway use DPSK (Differential Phase Shift Keying) for signal conversion. The signal form another internet will be divide and converted to reach the proper destination the main aim of the DPSK is to check whether the signal from the device is same as the signal which leaves the gateway. This Frequency Shift Keying (FSK) is a process of conversion and invention which invent the input signal from the devices. If the signal is impaired this Frequency Shift Keying (FSK) convert the signal into original format this

contain lower space for the data. Additionally, his contain high sensitivity which sense the signal quickly.

Yeonjoo et al (2018) experiments a LPWAN tracking platform based on SIGFOX Network as SIGFOX has very good short-range sensor object tracking system [ref]. In this paper, they have used SIGFOX to track an object which is located within certain radius. However, once the sensor is connected to SIGFOX network it will automatically publish its data and send it to the SIGFOX backend. In this LPWAN tracking platform, the main controller board was Arduino Uno board which transmit GPS data to SIGFOX backend. Additionally, call back message handlers, call back data handler and call back services were acknowledged. Moreover, the application server collects all the call back message from the SIGFOX network and certain operations will be performed based on it like sending real-time location or to store all the messages in the database. Author Laura and his team (2019) designed a wireless environmental monitoring system that transmits data via SIGFOX cloud for every 5 minutes. Sensor nodes are been placed in different places in the country to monitor the environmental changes. Moreover, to transmit all the data Bluetooth or ZigBee will not be suitable for long range communication. Mobile cellular technologies (3G/ LTE) consumes more power which will not be applicable for low powered sensors. So, for this scenario Low-Powered wide-area network (LPWAN) protocol such as SIGFOX have been used to transmit the data.

3.2.2 LORA

The long-range wireless communication can be established by LORA which a physical layer for long communication. For the efficient low power communication, the physical layer use frequency shifting keying (FSK) modulation. Lora technology is based in the chirp spread spectrum (css) of low-cost technology. This technique is derived from the spread spectrum modulation. Around 10 years the military and space communications are established by the Lora technology using Chirp spread spectrum.

The Lora consist of single base station for entire communication which covers hundreds of square kilometres. Additionally, LoRaWAN. Low-Power, Wide-Area Networks (LPWAN) which connects billion of devices in IoT.

Local Area Network Short Range Communication	Low Power Wide Area (LPWAN) Internet of Things	Cellular Network Traditional M2M
40%	45%	15%
Well established standards In building	Low power consumption Low cost Positioning	Existing coverage High data rate
Battery Live Provisioning Network cost & dependencies	High data rate Emerging standards	Autonomy Total cost of ownership
Bluetooth 4.0	LoRa	GSM 3G+ / H+ 4G

Fig 7: Lora over view

Local Area Networks are fit for enhancing the communication with personal devices. Cellular network fit in the application which required a larger data input for the high-power sources. LPWAN proposed a design for different sensors and application which send a data over a long distance with diverse environment. Furthermore, the LPWAN connects highest number of nodes over a large distance with high network security. Besides, this technology also agrees both one way and two-way communication for wider range of devices with low power technique. The LPWAN establish high security for the communications with AES encryption technology for the entire network communication.

3.2.3 NB-IoT

NB-IoT is Narrow band of Internet of things (NB-IoT). Based on the LTE (Long-Term Evolution) this technology can access cellular radio which is a LPWAN technology. This NB-IoT is mainly for establish the communication between the machine to machine communication in with low power, cost and data-rate. NB-IoT works with three different ways. Firstly, the NB-IoT is a wireless independent technology. Secondly, this technology can also works using GSM (Global System for Mobile Communications) finally, the NB-IoT can allocate a block in LTE base station for enhance communication. The main advantages of NB-IoT is power efficiency, low cost, reliable, wider deployment and international reach. The IoT technologies are mainly developed for saving powers on

using 20 billion connected devices, this technology run with low power so this will not take high cost for communication. Moreover, for efficient power saving this technology has buffering, channel estimation, Analog to digital conversation and digital to Analog conversion to establish better communication. This technology is more reliable which provide better quality and performance. Moreover, this NB-IoT technology has wider range of IoT connected application like monitoring of gas, parking monitoring, monitoring water, personal health monitoring, smart cites and industries. The security of data integrity and authentication services are also established over these techniques.

3.3 BLUETOOTH:

Bluetooth is a linking of electronic devices like mobile phone, computer and other devices. Bluetooth can be equipped in home, car, and offices and anywhere this helps to share the information between devices connected. Nowadays, the number of devices is incorporated with Bluetooth technology. The Bluetooth is a microchip which helps to transmit and receive the data with the frequency of 2.4 GHz bandwidth. One megabit for second is the time taken for the information sharing. Bluetooth used to work on the frequency band of 2,4 GHz bands. There is 3 level emission of power for the Bluetooth there are three classes of power depend on the range. The maximum Bluetooth range is 10 meters. it will be more efficient if the devices are in the short-range in a closed environment. Normally, Bluetooth technology works with the design of master and slave for data communication. Maximum up to seven slaves can connect over the signal master node for the data exchanging. The connected need to give request once they accepted then only the communication could establish. Another thing is, communication can only develop with the master and slave or slave to master. The communication cannot be done with the slaves.

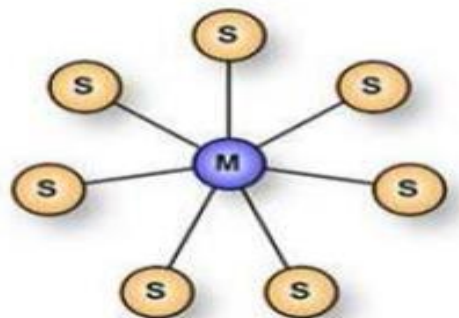


Fig 8: Bluetooth node

BLE:

Bluetooth low energy (BLE) works with low power and low energy consumption. Normally the Bluetooth works with the limited range for communication and sharing resources. The Bluetooth low energy also the same process with the low-power wireless technology. BLE technology has a battery range of 2.0 days and 14.1 years. The beginning of BLE has happened though additional low-power wireless explanations, such as ZigBee, 6LoWPAN or Z-Wave, which has multimode networking. Nowadays, BLE is used in various fields like HealthCare, smart cities, smart houses, industries and security with low power and energy. The Bluetooth technology only has the masters' slave model, but, the BLE has a master, slave, master/slave design. The master can connect to seven slaves. Additionally, the master can act as a master as well as a slave for connecting various slave node, which also inclines the communication nodes to form a network.

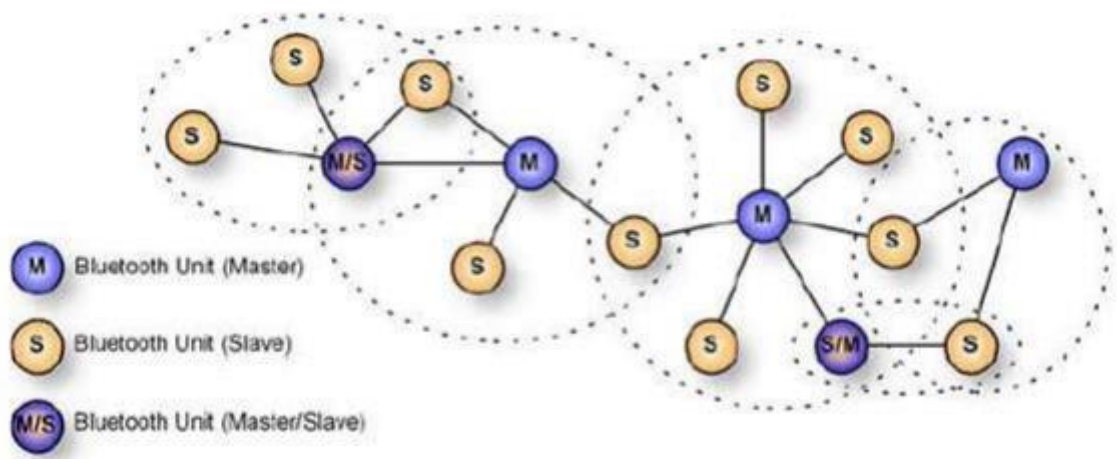


Fig 9: Bluetooth low energy

BLE security is more advanced than Bluetooth, which has various security services for the connected devices over the network. The BLE has two modes of security LE security mode one and LE security mode 2. Which has the encryption of 128 bits AES and Cipher Block Chaining-Message Authentication Code (CCM) each mode security has different levels of authentication during the connection of slave to Master. During the connection establishment, security management protocol takes place during the message transmission between the paired devices.

3.4 GEOLOCATION-BASED MOBILE APP DEVELOPMENT

(Kerby, 2017) researched on Mobile app development that uses Geolocation services, the author discusses the importance of location-based mobile application and how the technology has been transformed. By using modern technologies, it is possible to track a person address and where he travels with his street etc. [change sent]... For developing a geolocation-based mobile application,

there are two

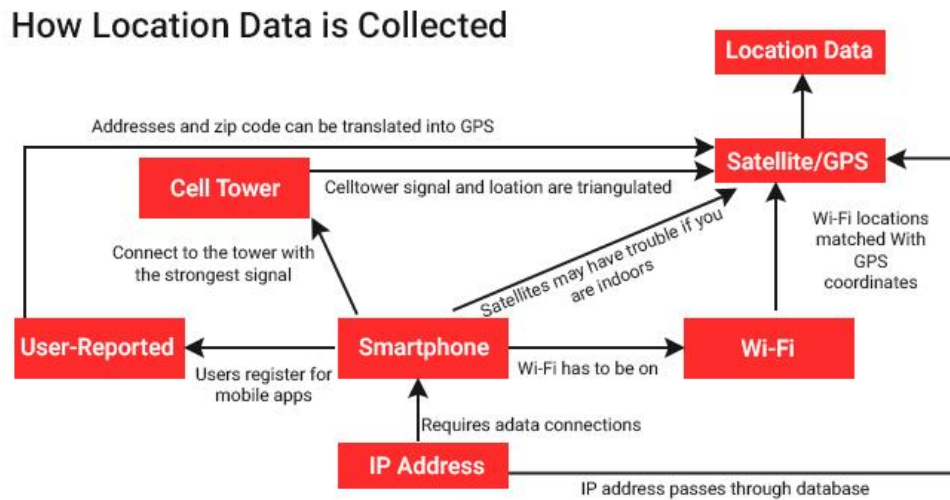


Fig 10: collection Geo-location data

3.5 CLOUD PLATFORM

Cloud computing provides working spaces as services over the network, to use their resources with a limited cost (Kakkinos et al., 2013). As day by day, technologies are being upgraded. We can get a small office setup environment by setting our machines with required configurations we need. Moreover, many companies compute and store their data on a public/ private cloud. Several IoT services are available that provides many

features for the user to store, analyse and visualize their data, from the collected data and provides many more features.

AWS IoT

Amazon Web Service is one of the leading IoT service providers. However, it is a little costlier than other IoT service providers. AWS IoT is available for both edge software and cloud services (Tudip, 2019), that allows developers to collect the data from the sensors/devices and pass the data to the Amazon cloud platform for visualization and analysis to make an intelligent decision.

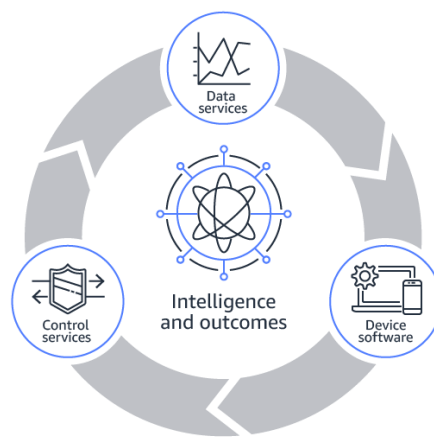


Fig 11: AWS IoT

3.5.1 AWS

AWS IoT cloud services

To connect the IoT devices to the cloud platform applications, AWS provides many cloud services such as,

AWS IoT core:

AWS IoT Core cloud service that allows IoT enabled devices to connect and securely transmit data with other devices. AWS IoT Core can also use AWS services like AWS S3, Amazon Cloud Watch, and AWS Lambda. It can connect hundreds of devices and transmit thousands of messages to other devices reliably and securely. Moreover, the applications can communicate with all the AWS IoT core enabled devices, even when they aren't connected. It can securely organize and monitor remotely anywhere.

Amazon Web Services – Cloud Watch

Amazon Web Services (AWS), provides web service access to Amazon's cloud infrastructure. Amazon Elastic Computing cloud- EC2 is the most popular web service, which provides resizable compute capacity as a service that is, the user can integrate his hardware/ software requirements for rent over a period of time (Kakkinos et al., 2013) Amazon CloudWatch has an inbuilt service that monitor's applications data based on the logs, metrics, and events to perform the actionable insights. CloudWatch also detects unusual changes or malfunction of the application and troubleshoot that issues to keep the applications running smoothly.

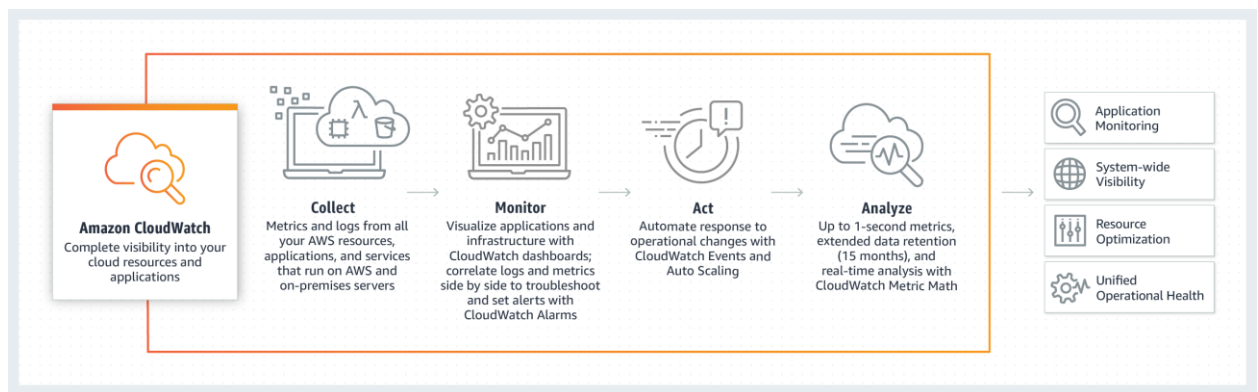


Fig 12: Cloud Watch working

(Rai et al., 2018) developed a prototype for women safety that takes real-time location from the GPS sensor and sends it to the cloud database. Moreover, a notification will be sent to the parents so, by logging into the mobile application, they can see the recent location of the user. (Rai et al., 2018) Implemented using Raspberry Pi and GPS module for collecting the geolocation coordinates and store them in a database that will be running in the Amazon instance. T1 micro Amazon EC2 instance running on Ubuntu 14.04., AWS CloudWatch was used to visualize the user location and act as a notification service for sending an emergency alert to the contacts. Similarly, Patel, K. & Bhatt, N. (2019) developed an IoT enabled wearable camera which will be directly integrated to AWS S3 bucket for storing all the video recording. Amazon S3 (Simple Storage Service) bucket is public cloud storage, which allows storing an object and can give access privileges for the stored object in a bucket (Rouse, 2017). User can interact with the S3 bucket via AWS

command Line interface, or API's can be integrated. Patel, K. & Bhatt, N. (2019) uses AWS API's for setting up the access logs and link to the respective bucket, so when the Wearable camera is triggered by the user, it starts recording video and transmits to S3 bucket.

3.5.2 IBM WATSON IOT

IBM is a leader in the Forrester Wave an Industrial IoT Software platform, IBM Watson IoT is a managed service that is hosted in the cloud for secure connection, management and processing of IoT data. IBM is a cloud platform with different features which is a cloud computing platform with hybrid cloud model. The IBM cloud has different services provided for the users such as Internet of Things, security, Data and analytics, Networks, application services, and many more (Harvey, 2017).

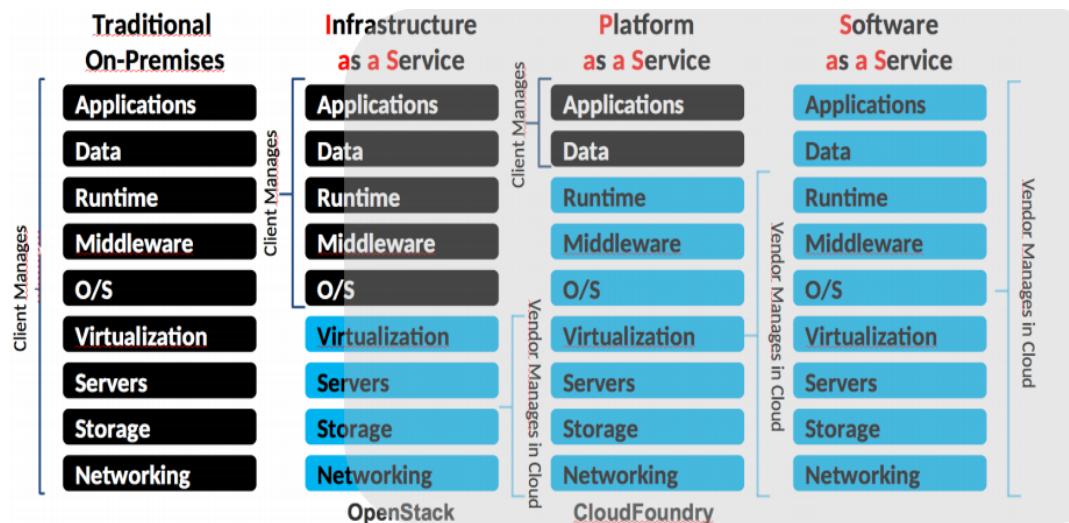


Fig 13: IBM Watson IoT Architecture

IBM has three main services, Infrastructure, platform and software as a service. In the infrastructure set of hardware, software, servers, operating system and storages are taken place in that infrastructure services, platform has a set of tools and software service has set of designs for the users

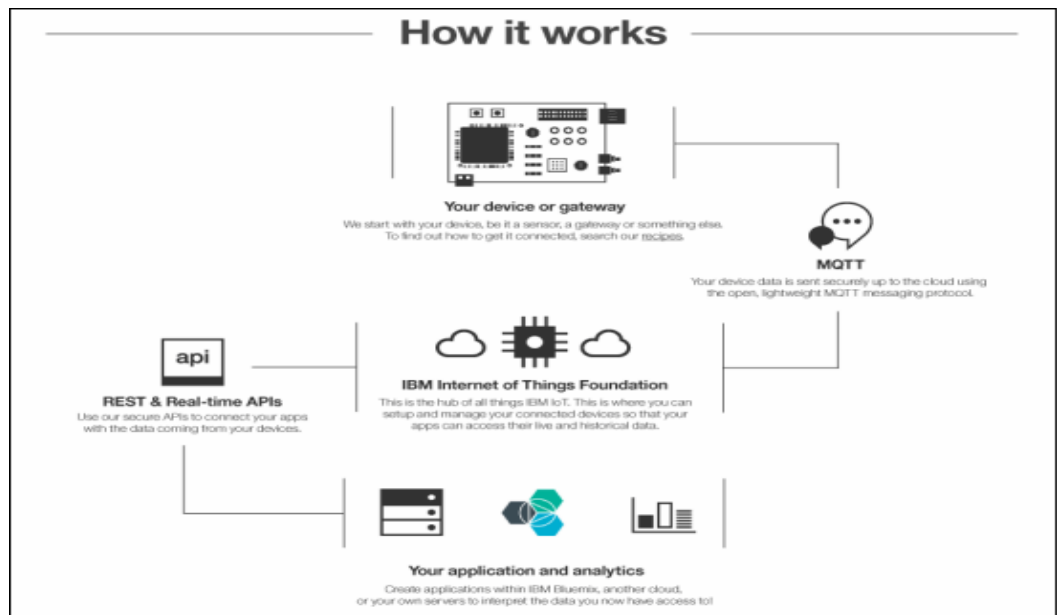


Fig 14: Working of IBM Watson IoT

In that Internet of things platform is one of the services in the IBM cloud which mainly helps to connect and communicate with the devices over the network and additionally, help to establish communication and interconnection with the applications and tools. The IBM enhance the connection between the devices, applications, sensors, gateways for sharing the data the communication is also developed by the MQTT protocol to the IBM cloud. Moreover, the data has gather using REST APIs from the particular application then the data is used for analytical purpose or other purpose for the application.

3.5.3 GOOGLE – Firebase

Google cloud platform offers Web Service and Cloud Computing, including data storage, data analytics and machine learning kit. Moreover, GCP provides Cloud IoT core for high security which is cheaper in cost than AWS.

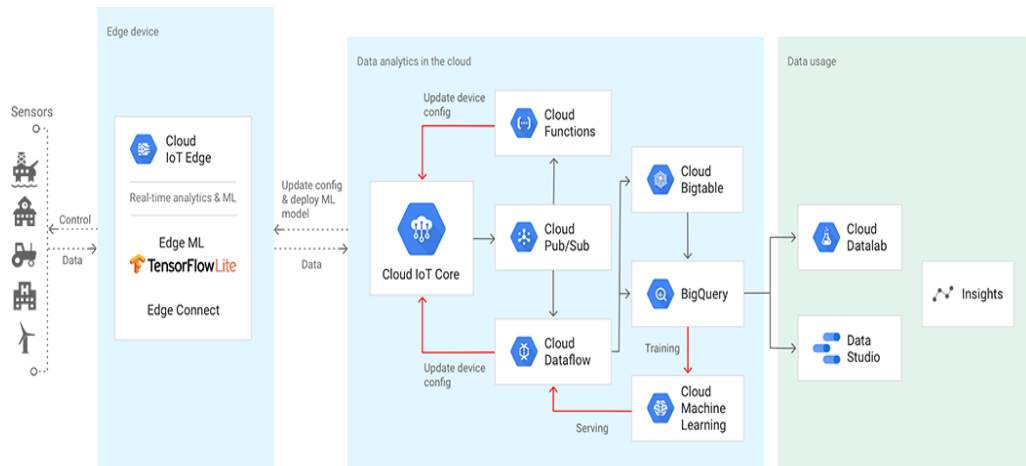


Fig 15: Google Firebase

GCP can connect, manage and consume data from numerous of connected IoT devices. Moreover, it helps developers to collect, process, analyse, and visualize real-time IoT data from the connected devices. Cloud IoT core comes with the Google cloud data analytics feature in it which enables the user to stream the IoT data for further visualization and prediction (Tudip, 2019). Google IoT core runs on the server less infrastructure, it scales manually when there are any changes in real-time data (Tudip, 2019).

Firebase is a web and mobile application development platform for backend as service in the cloud, including user authentication, hosting, and real-time database. Moreover, firebase cloud system provides SSL encryption data transmission. Firebase real-time database is a NoSQL type database, moreover it has one of the most advanced and secured databases which is an API that Syncs application data across all mobile and web platform such as Android, iOS, and Web devices and stores the data on Firebase's cloud. Firebase is a toolset to improve and build app with real-time storage, authentication, analytics, database, and hosting. Moreover, in the android Studio, firebase plugin can be directly synced to transfer and retrieve real-time data from the cloud. The company provides client libraries that enable integration with Android, Swift, Node.js, java and java Script (Wu-Jeng Li et al., 2018). Hosting will be completely maintained and operated by Google to host the server. Client SDK's has Firebase interact tools with which the backend service establishes without any middleware between the app and the service. So, by using the firebase database, to query the database the code will be written in your client app.

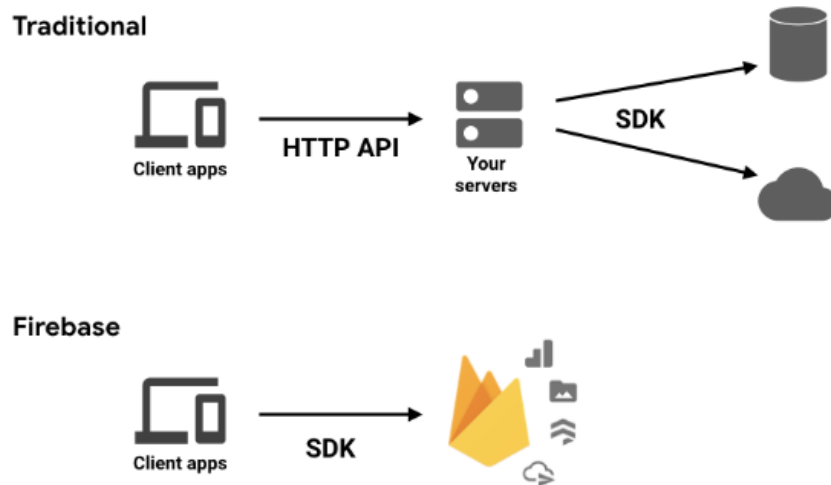


Fig 16: Traditional vs Firebase

3.6 SMS API

Twilio is a Programmable SMS API (Application Programming Interface) platform which is used for sending SMS around the world. All these powerful API tools can communicate or send message to different social communication platforms like SMS, Voice, WhatsApp, Facebook Messenger and more. Using Twilio's REST API, you can send outbound SMS message from the Twilio phone number we get. Initially, after creating a Twilio

3.7 PYCOM

The main motto of Pycom is to help people who like to develop and connect things fast, Simple and in efficient way. The first product of Pycom was WiPy, was launched on April 2015. Over 1,300 people not only keen on innovative products but also clearly required enterprise grade, fun and easy to program the Pycom board. Initially, one of the Co-founders were busy in building their first product called KS devices, one evening they have spotted the campaign, then it was later discovered and introduced as WiPy to their team as one of the future Py devices.

It is necessary to explain the "Pycom" terminology. Firstly, "Py" is a diminutive of python particularly micro Python, which is superfast Scripting language. Moreover, micro

Python is easy to learn for new beginners and at the same time it is easy-to-program with faster processing speed. On the other hand, “Com” part simply stands for “Communication” e.g. connected devices that communicate via a network. After the launch of their first product, they want to give developers/ student a choice of connectivity platforms. They can choose their communicating option through which they want to connect the IoT devices and transfer their data. However, IoT market has evolved dramatically in last five years [1].

The co-founders with a strong blend of IoT Hardware and services capabilities, wants to help others who are interested in technologies to build and connect the devices wherever they want. As days gone Pycom have built many devices with different network combinations such as,

- FiPy - Wi-Fi, Bluetooth, LoRa, Sigfox and dual LTE-M (CAT M1 and NBIoT).
- SiPy - Wi-Fi, Bluetooth and Sigfox.
- gPy - Wi-Fi, Bluetooth and dual LTE-M (CAT M1 and NBIoT).
- LoPy - Wi-Fi, Bluetooth, LoRa and Sigfox.
- WiPy - Wi-Fi and Bluetooth.

Pycom Expansion boards with inbuilt sensors

- Pytrack - GPS and accelerometer.
- Pysense -Temperature, Pressure and Humidity.
- Pyscan - accelerometer, light sensor and RFID-NFC.

Fipy is one of the most powerful microcontroller which has powerful computation that uses Ultra-low power usage. Dual processor and Wi-Fi radio system on chip Espressif ESP32 Soc .Networking processor handles the WiFi connectivity and the IPv6 stack. Main processor is entirely free to run the user application

An extra ULP-coprocessor that can monitor GPIOs, the ADC channels and control most of the internal peripherals during deep-sleep mode while only consuming 25uA. Fipy is using SHA, MD5, DES, AES encryption technique.

4 DESIGN

4.1 PROPOSED SYSTEM DESIGN

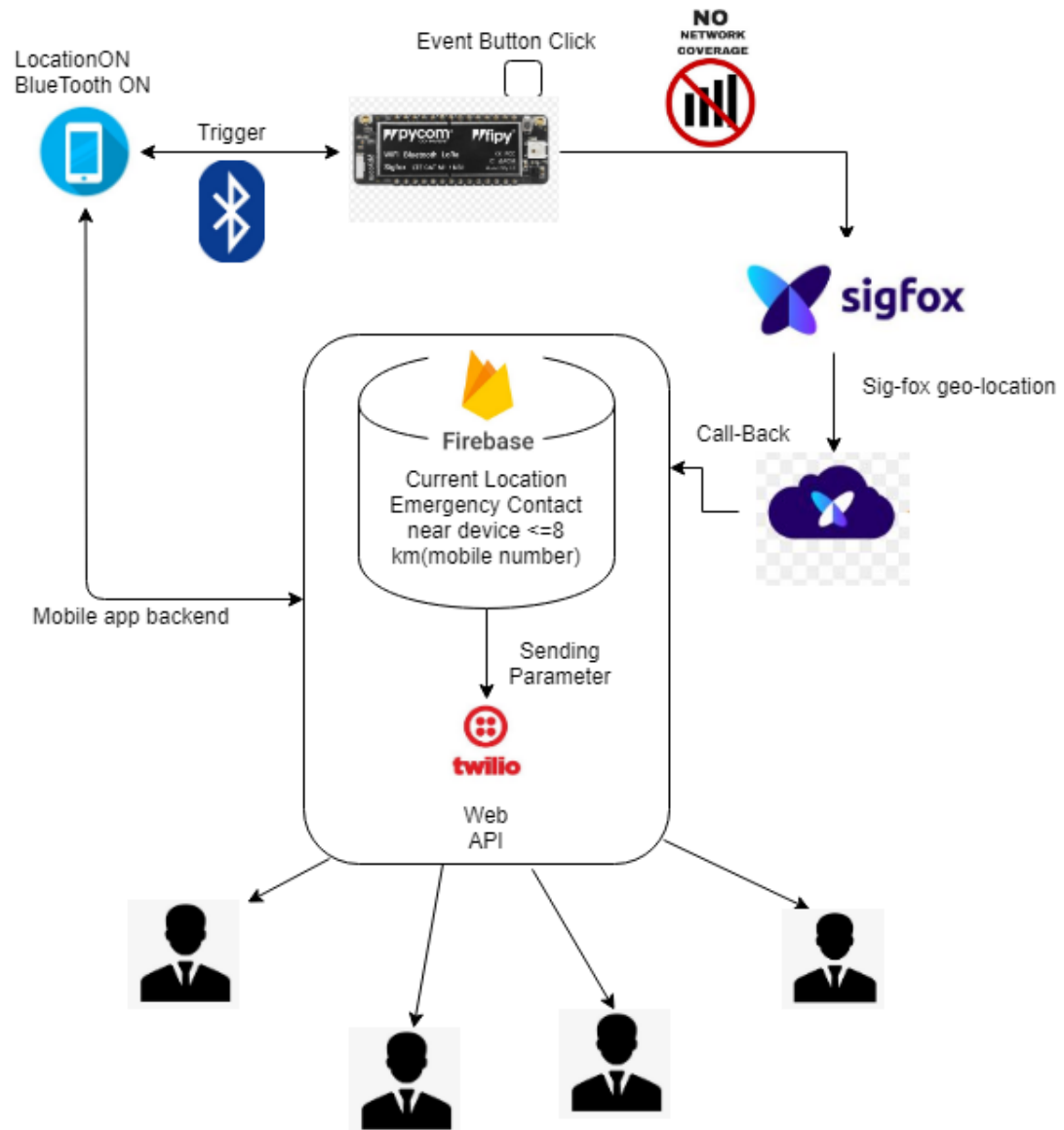


Fig 17: System Design

4.1.1 WORKING MODULE

A trigger is an event that will be generated to which the actions will perform. A trigger/event can be, form a button or any sensors, based on the trigger the action will be performed. Many existing products and proposed models related to my proposed system used different kind of sensors (Scream, sweat, motion, and so on) to trigger an event. Nandhini (2018) researches on the different types of trigger and action methods. Most of the papers have different trigger events but the action phase is same, sending SMS through GSM with real-time location to the pre-defined emergency contacts. The problem with the existing proposed systems are same as mentioned in the (section 1.2). If the women is far away from home, their parents or friends will not able to go and help them during their emergency situation, if the women gets any help from the people around them would be more helpful for them. In the proposed system of this thesis, the basic button click has been used to activate the SOS alert trigger the reason for this is, this thesis mainly focused on the action part that is. On the other hand, one of the most commonly used methods for send alert SMS is via GSM module for instance, consider that a women is in some rural location where there is no proper network coverage. If they are in an emergency situation, SOS alert SMS cannot be sent to the pre-stored contacts. So, to overcome this two main problem in the existing system, research has been done for making a smart alert system to the nearby devices based on the victim's current location.

Once the user has clicked the emergency button, the trigger will be generated and send to Mobile application via Bluetooth as well as a trigger will be sent through Sigfox module (fall back module) which is inbuilt in the Fipy module. Moreover, once the button is clicked by the user, Sigfox module will send the Geolocation of the Sigfox device, which is an inbuilt service that can send the Sigfox device latitude and longitude (approx.) to the third-party servers with the help of call back function. On the other hand, a trigger which will reach the Safety band mobile application has to make the backend action performed.

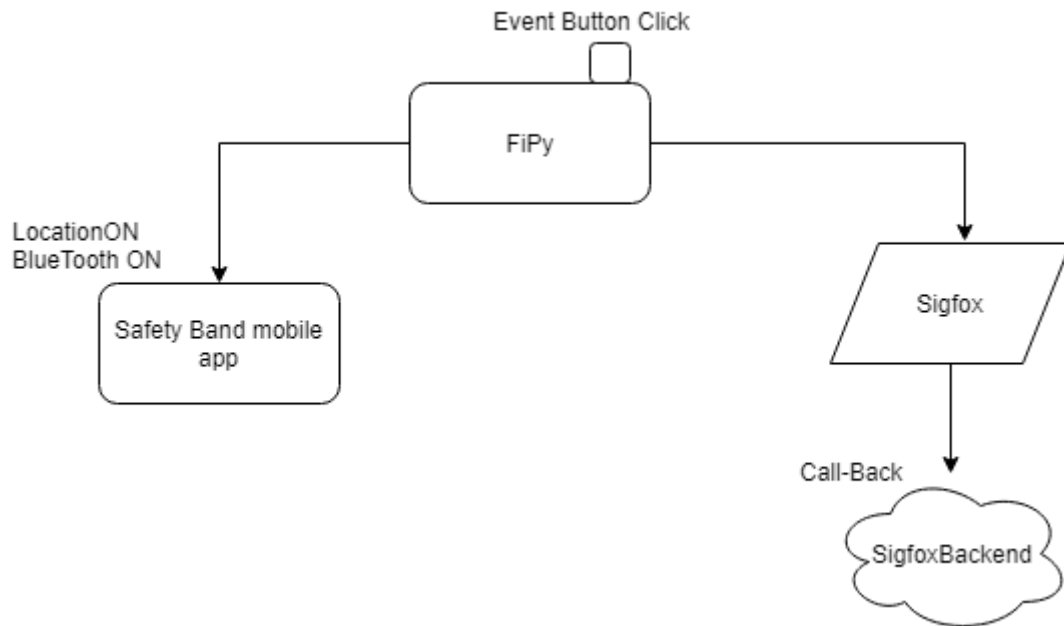


Fig:18: Trigger event sends to Mobile Application and Sigfox

4.1.2 Trigger sends to Mobile application

Firstly, the user have to install the Safety band Mobile application and have to do some basic setup like the account number, which will be the primary key in the database. Next, the emergency phone number should be added, to send the SOS alert message to their mobile number with real-time location. All the number added will be stored in the firebase database, so each time when the mobile application is on, the current location of that user will be updated in the firebase database. The user have to connect the Safety Band with their mobile application, by turning on the Location and Bluetooth service on their mobile phone. Once the location service is on, the user current location will be updated in the database from then for every 30 seconds, and the updated location will be notified in the notification bar. When the user feels any distress or an emergency situation, by clicking the emergency button on the band, a trigger will be generated and sends to the mobile application via Bluetooth. Once, the mobile application receives a trigger from the Safety Band, and a filtering process will be done in the Android backend. At first, the users current location and their Emergency Contact numbers (which is added in the mobile application) will be taken and then based on the user current location, it will search for the active devices available within 8km (this is not the standard search, it can be changed) and retrieves their number from Firebase real-time database. As the firebase API, syncs with the android application, data retrieval from the Firbase database is simple. After retrieving all the emergency contact and near devices number from the database, the query

data will be sent to the application URL (/locationalert) in POST method. The data has four parameters (Latitude, Longitude, queried numbers and SMS msg)

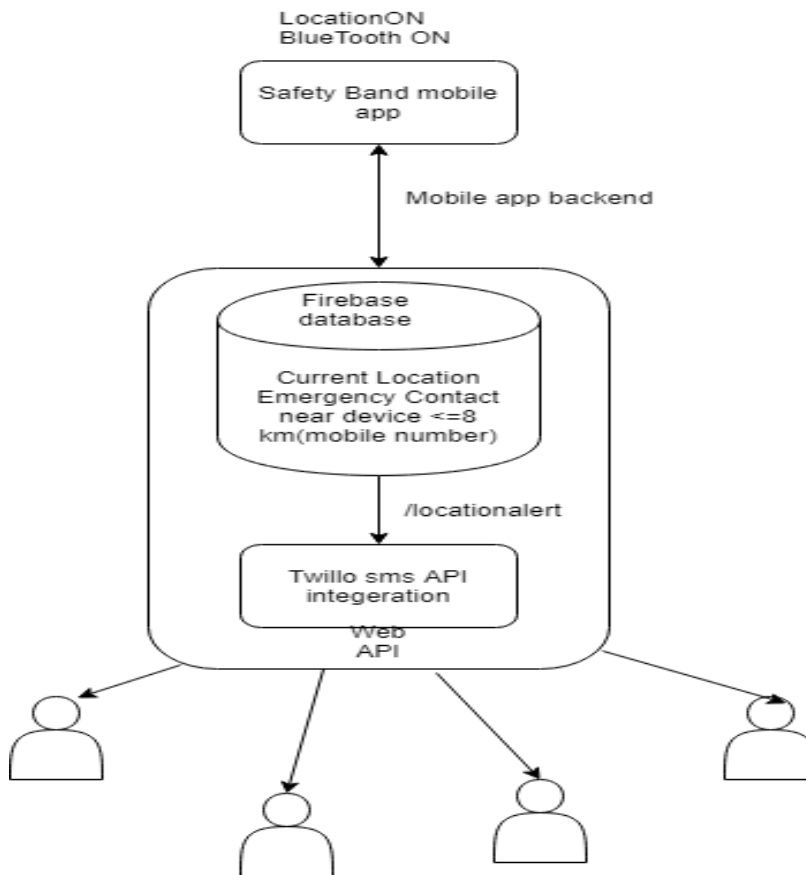


Fig19: Filter flow of Mobile application

4.1.2 TRIGGER SENDS TO SIGFOX

The emergency event will be triggered at the same time for both Mobile application as well as through Sigfox. Sigfox is a fall back module, in the case when the user is in some isolated place where there is no network coverage then they could not send an SOS alert. During the research, many proposed system, are using GSM module to send SMS, if the system fails there was no backup alert system provided. Sigfox has good signal coverage in all over Europe, especially in Ireland, this is one of the main reason for selecting Sigfox for this project. So, when the user clicks the emergency button, the trigger will be sent from both Mobile Application and Sigfox. The Sigfox device will send its geo-location points to the Sigfox backend. Through call back the location data, will be sent to Firebase hosting page, where the Web API is written to integrate with Twilio SMS. The data has two parameters (Latitude and Longitude). If the trigger comes through Sigfox, the same filtering process will be done on the Web API call. Based on the latitude and longitude

sent from the Sigfox the filtering will be done and filters the active devices (from the database) within a certain radius and send the emergency alert message to the filtered mobile numbers with the user's current location every 1 min the location update message will be sent to the end-user.

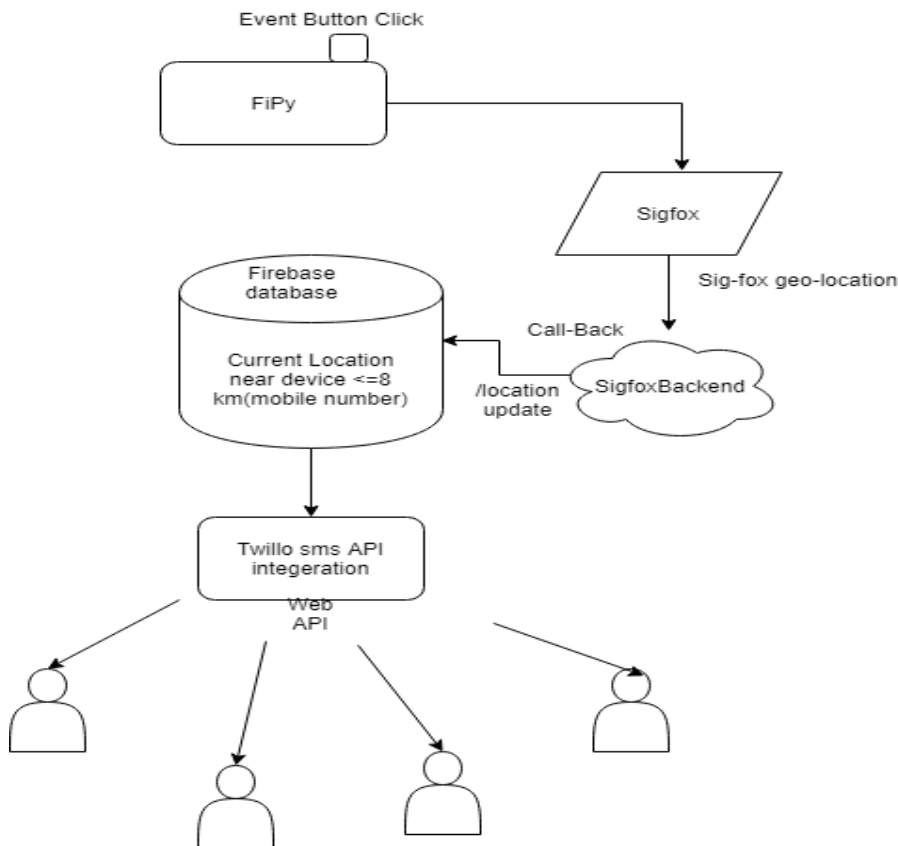


Fig:20 Sigfox Flow

4.1.3 Twilio Integration

This web API phase where all the data will be received, this web API will be deployed at web hosting in Firebase, Initially, all the required tool for firebase will be installed and initialized in our local PC. Firebase credentials, service account project ID and databaseURL are given to access the database. Next the Twilio credentials are given, by using Twilio API the SMS are sent to the queried numbers.

By POST method both the modules (Mobile APP and Sigfox), will be sensing their data. Mobile application will send the queried data and Sigfox will be sending the geo-location data. Based on the queried parameter that has been received by the API will be checked, if the query length is greater than equal to 4 parameters then, it is the data came from

(/locationalert), so here only Twilio SMS API integration will be called. If the condition fails, then the Sigfox Web API integration will be called. Based on the Sigfox geo-location, the database will filter the near active devices and quires all the near devices number. Next, the Twilio API services will be called and for all the queried numbers Alert SMS will be sent through Twilio.

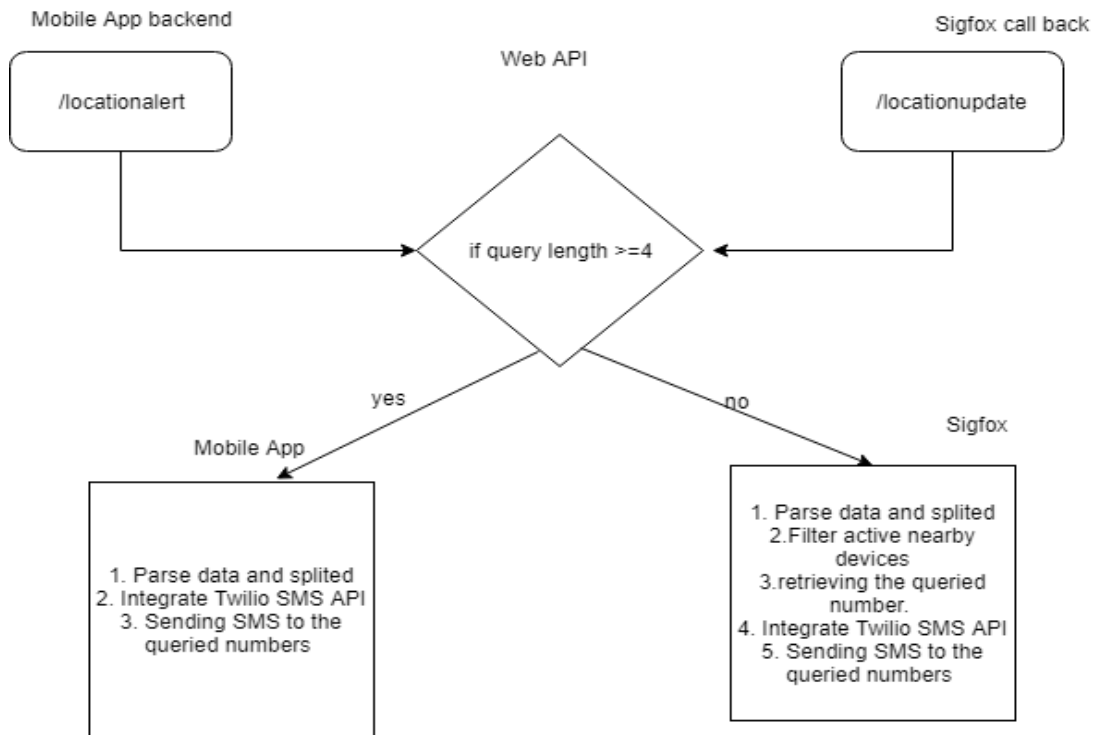


Fig 21: Twilio Integration

4.2 HARDWARE/ SOFTWARE SETUP

4.2.1 PYCOM FIPY/ EXPANSION BOARD

- To upload the programs and run them on Pycom devices, few suitable tools and setup have done. Before that, suitable drivers should be installed and updated, for Pycom to function correctly. Download the drivers for Windows from GitHub and save the file.
- There are two ways to connect your board to your computer either via USB or Serial connection. Before connecting to the Expansion Board, the firmware and drivers should be updated.
- Navigate to Control Panel a Device Manager, in other device section, we can see “Expansion Board 3” in the dropdown menu. Right-click on it and select Update

Driver Software. Select “**Browse my computer for driver software**” option and navigate to the path where you have downloaded the driver.

- After the installation, windows will display a popup message stating successful drivers update. Navigate back to Device Manager, and in the port menu, we can see the USB port has detected expansion Board 3.

Updating Firmware

- The firmware update is one of the important basic step, the reason for this is Pycom developers would constantly making improvements and adding new features to the devices.
- Latest firmware DFU file and Zadig – an Installer tool and DFU Firmware has been downloaded for Expansion Board 3.
- Firstly, open Zadig and in USB ID box we have to set the Expansion Board 3 PID (0xEF99) bootloader mode.
- libusbk drivers will be installed for Expansion Board 3.

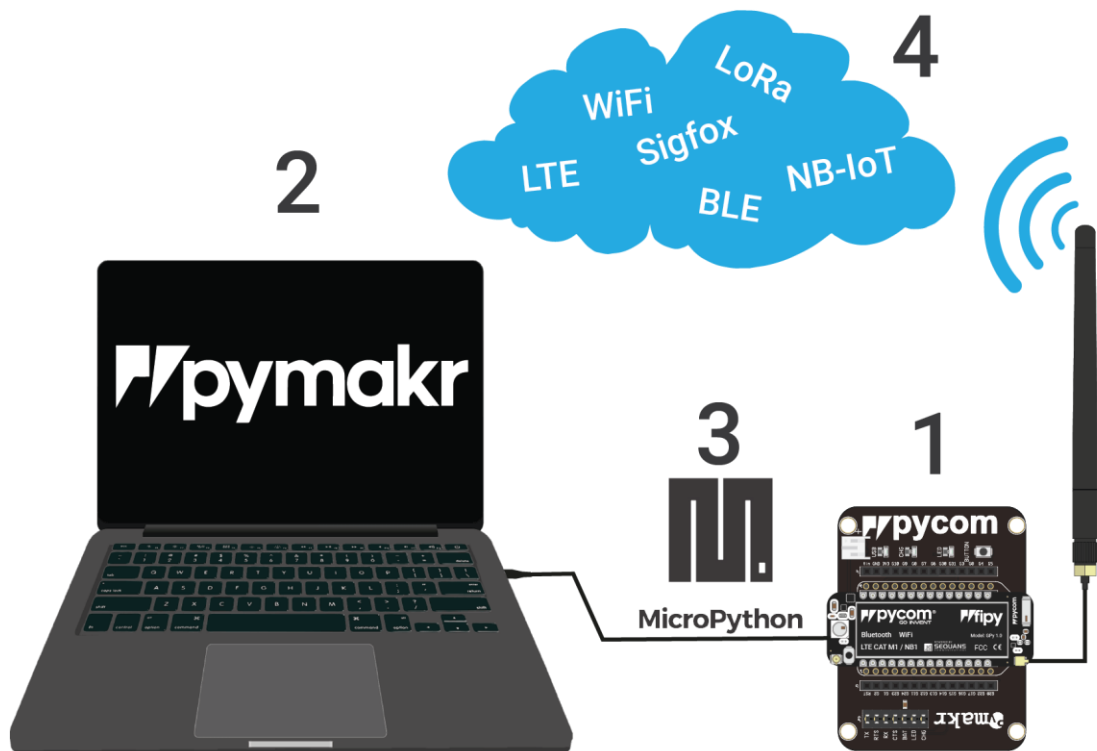


Fig 22: over all Pycom setup

Atom IDE

- Firstly, Atom IDE was downloaded and installed. Then navigate to Install Page to install Pymakr plugin, via Packages → install Packages → Pymakr (official pymakr plugin).
- By installing Pymakr, it adds the REPL console to Atom, that connects Pycom board and runs the code on the board. REPL (Read Evaluate Print Loop) is an interactive terminal that allows the developers to run and test their codes directly on the device.
- Pycom boards can be connected via serial USB, and the COM port can be manually entered in the global setting page. Now the Pycom boards will be connected to the Atom IDE.

4.2.2 SIGFOX

Sigfox is a Device-to-cloud communication system, which has inbuilt Sigfox (Low Power Wide Area Network) radios which connects to their operator network. Pycom has an inbuilt Sigfox module which comes with two years subscription connectivity free. To get Sigfox device ID and PAC latest firmware should be updated “Pycom firmware updater”.

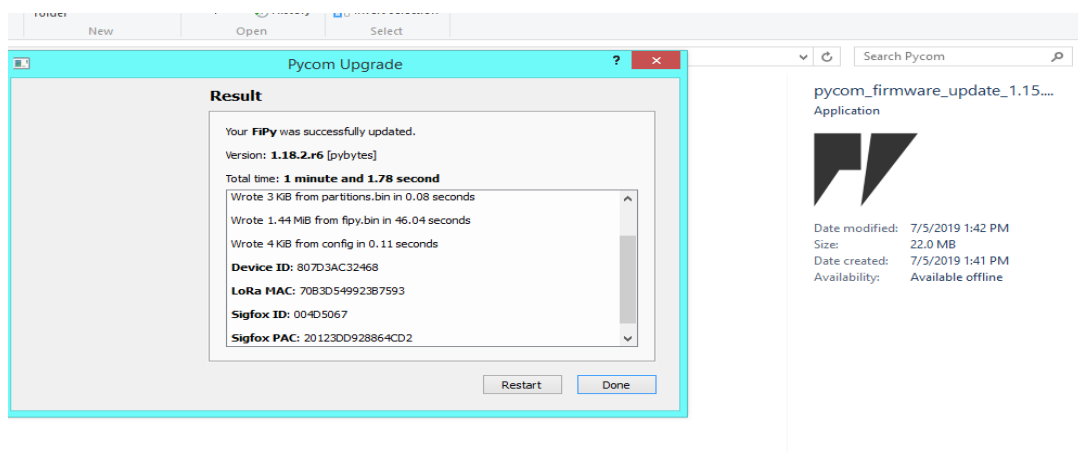
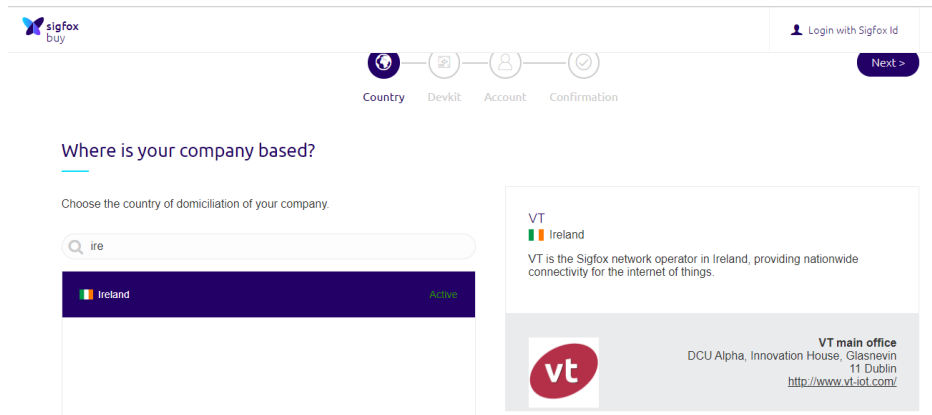


Fig 23: Firmware Update

Creating account at Sigfox backend

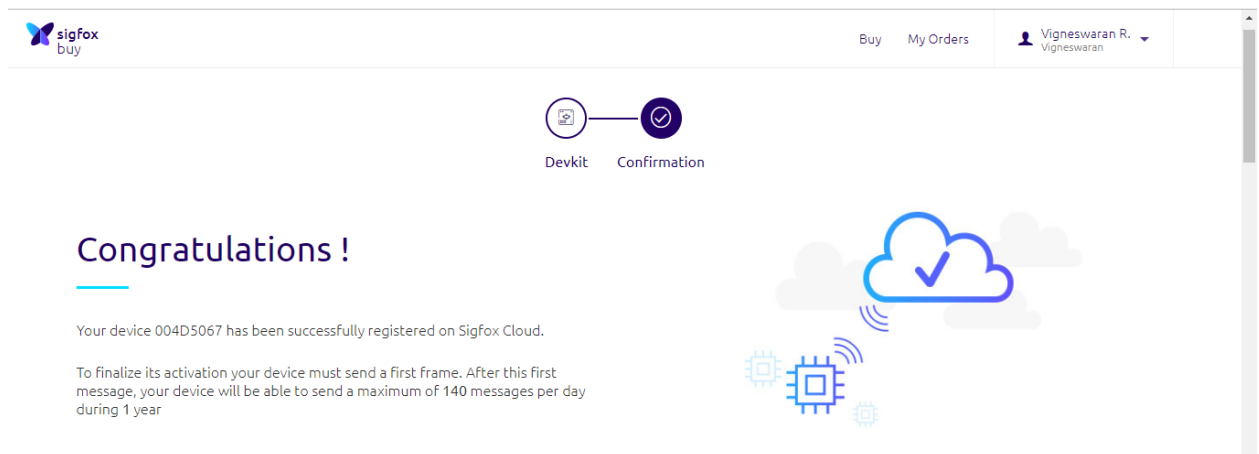
Firstly, Sigfox backend is registered. VT is the Sigfox network operator in Ireland, providing nationwide connectivity for the internet of things.



The screenshot shows the 'Country' selection step in the Sigfox account creation process. The user has entered 'ire' in the search bar, and 'Ireland' is selected. The page also displays information about VT, the Sigfox network operator in Ireland, including its main office address and website.

Fig 24: Creating Sigfox account 1

Next step is activating the Devkit, once the device ID, PAC (which we got in the firmware update page Fig 22) and other basic details is entered the Pycom Sigfox device module will be activated with the subscription connectivity free for 2 years.



The screenshot shows the 'Confirmation' step in the Sigfox account creation process. The page displays a 'Congratulations!' message and instructions for device activation. The user's device ID 004D5067 has been successfully registered on Sigfox Cloud. The page also displays information about the device's activation status and the number of messages it can send per day.

Fig 25: Pycom devkit Activation

Moreover, the PAC ID which was used to register the device is not valid, so that the new PAC will be generated for this Sigfox ID. To get the new PAC, login into Sigfox backend and navigate to device tab → select device number, this new PAC will be used in the code.

4.2.3 PYBYTES

Pybytes is an IoT Middleware platform that empowers and grant full control (Pycom devices) to the developers. By using Pybytes, developers have full control over the Pycom device and data management. We can add our Pycom device and integrate them with Sigfox by giving the API access credentials (API access Login and password). The data can be visualized. Moreover, Pybytes also has Firmware over the Air (FOTA) which has enhanced security updates.

Features of Pybytes:

- Data Visualization.
- Smart Notification.
- Terminal.
- Device geolocation.

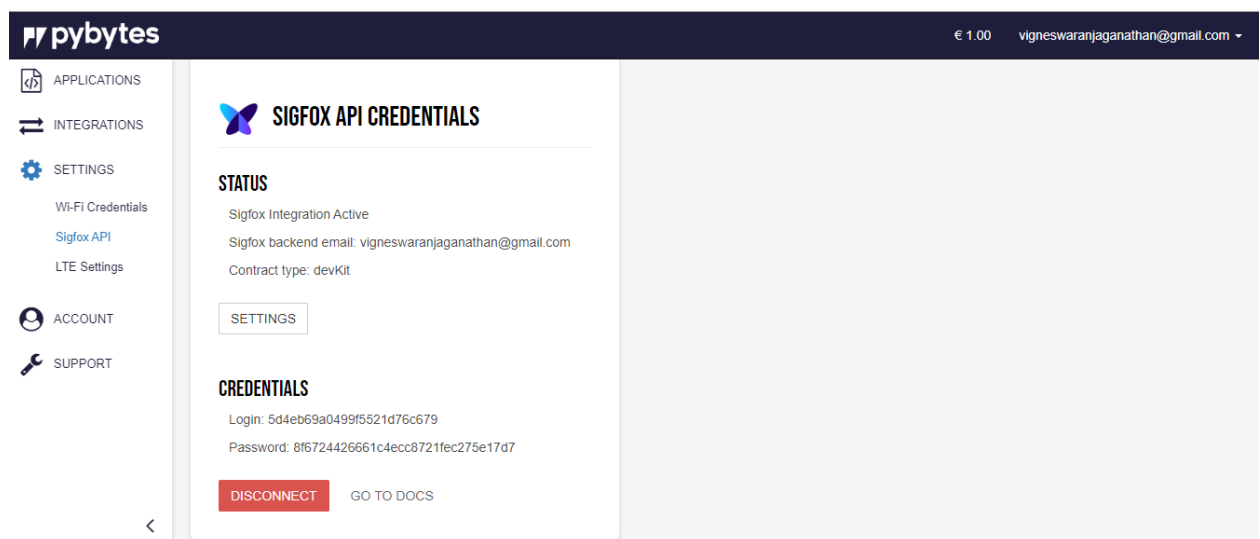


Fig 26: Pybytes API credentials

4.2.4 TWILIO SMS API SETUP

- First, the Twilio account is created.
- Initial free account balance of \$20 will be given.

- In Twilio free trial account, we cannot send bulk SMS as well as to access the Twilio external API from Firebase, the trial account will not be supported.

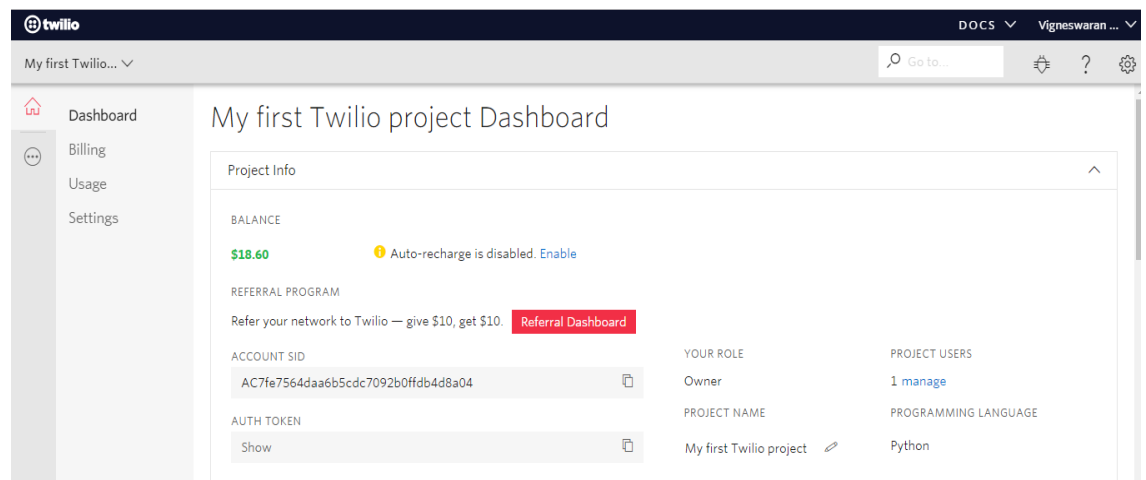


Fig 27: Twilio SMS API setups

- Upgrade has been done, by navigating to Twilio → Upgrade page, minimum \$20 to \$200, Moreover, for each country, there are different pricing for SMS, voice etc.,
- SMS pricing is based on the destination and type of message you're sending. Pay-as-you-go plan is chosen. To send SMS, it costs \$0.0700 and to receive \$ 0.0075.

4.2.5 ADD FIREBASE AND ANDROID STUDIO

- Create or signup with Google.
- Installed Android Studio for Windows and set up a device or emulator for run and test android app.

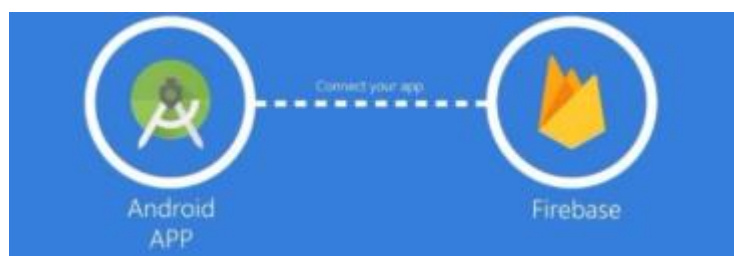


Fig 28: Firebase and android studio

- Next step is to add Firebase to our Android Studio project. Navigate to Tools → Firebase to open Firebase assistant window.

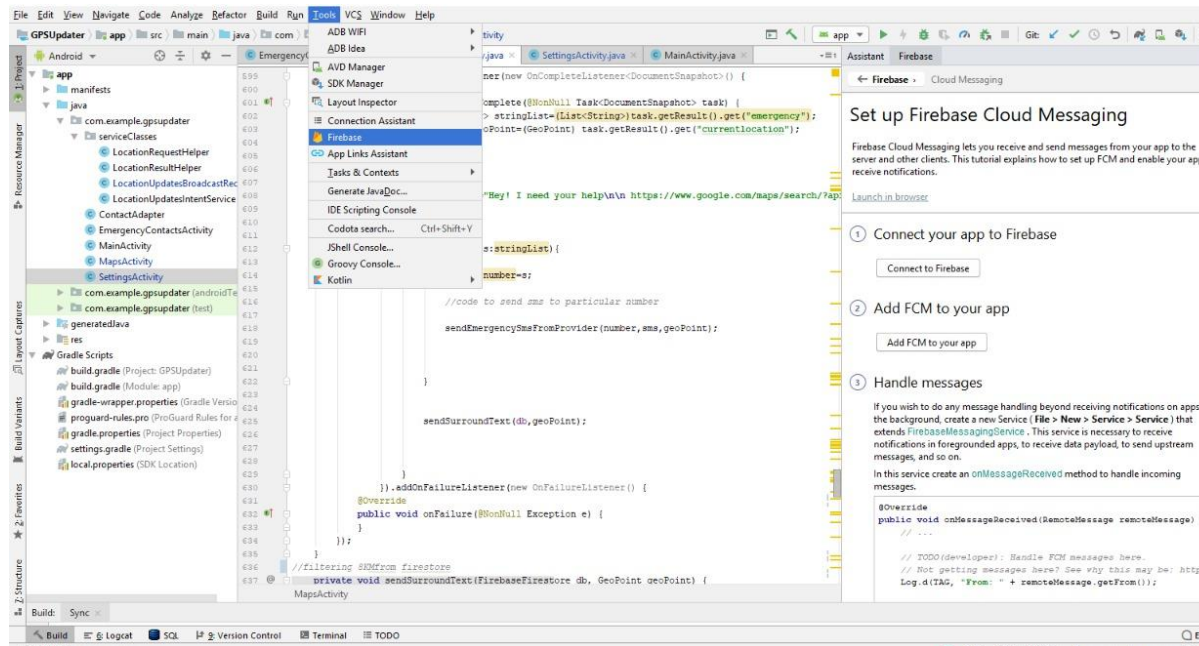


Fig 29: adding Firebase in android studio

- An window will be popped up on the left corner of the screen, then by clicking it will provide tutorial links for the setup extra tools.
- Next to **Connect to Firebase** to register our App with the project created. Moreover, all the plugin and libraries should be up-to-date.
- By logging into the firebase console, we can view our created project log and other features can be utilized, such as storage, hosting, analytics, MLKit and so on.

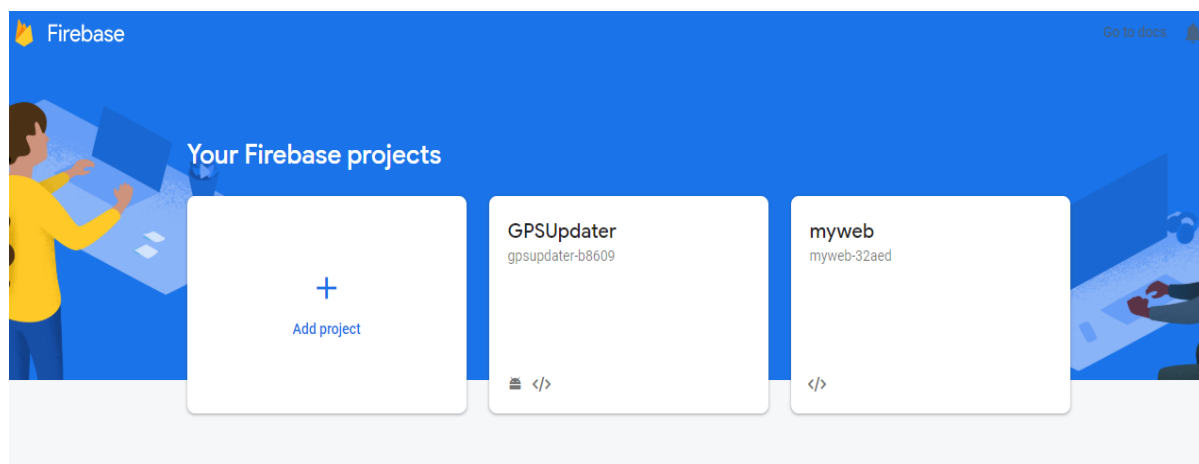


Fig 30: Firebase Projects

- From the Android studio IDE, app is launched to send verification to Firebase, and we can view the logs in console dashboard.

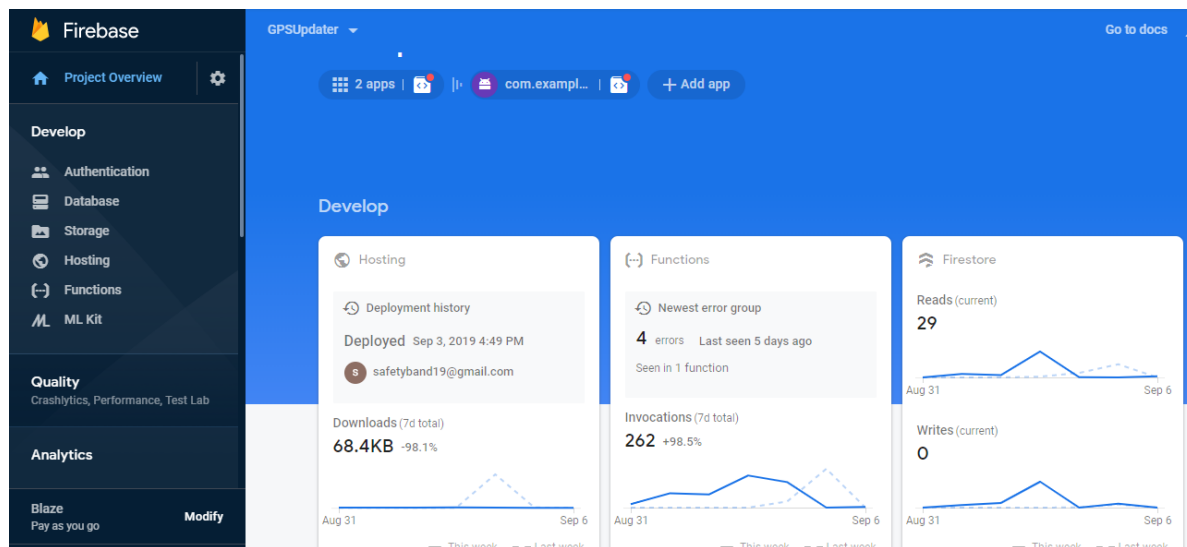


Fig 31: Firebase dashboard

- Secure the Cloud Firestore database, only application server (Node.js) have authentication to still access the database. Moreover, there is an option to set the location where the database has to be stored.
- To setup the development environment, first Node.js has downloaded and added path for Web API hosting.
- Firebase needed tools will be downloaded, “npm install firebase-admin --save”

```
? Which Firebase CLI features do you want to set up for this folder? Press Space to select features, then Enter to confirm your choices. Functions: Configure and deploy Cloud Functions

=== Project Setup

First, let's associate this project directory with a Firebase project.
You can create multiple project aliases by running firebase use --add,
but for now we'll just set up a default project.

? Please select an option: Use an existing project
? Select a default Firebase project for this directory: gpsupdater-b8609 (GPSUpdater)
i Using project gpsupdater-b8609 (GPSUpdater)


=== Functions Setup

A functions directory will be created in your project with a Node.js
package pre-configured. Functions can be deployed with firebase deploy.

? What language would you like to use to write Cloud Functions? JavaScript
? Do you want to use ESLint to catch probable bugs and enforce style? No
✓ Wrote functions/package.json
✓ Wrote functions/index.js
✓ Wrote functions/.gitignore
? Do you want to install dependencies with npm now? Yes
```

Fig 32: Firebase Initialize

- It will download all the needed tools for Firebase, By selecting the project

 **Firebase**

Project Overview

Develop

Quality

Analytics

Blaze

Authentication

Database

Storage

Hosting

Functions

ML Kit

Crashlytics, Performance, Test Lab

Pay as you go

Modify

GPSUpdater

Hosting

Go to docs

V

Dashboard

Usage

gpsupdater-b8609 domains

Connect domain

Domain	Status
gpsupdater-b8609.web.app Default	
gpsupdater-b8609.firebaseio.com Default	

gpsupdater-b8609 release history


Status	Time	Deploy	Files
★ Current	Sep 3, 2019 4:49 PM	 safetyband19@gmail.com fea144	3

Fig 33: Firebase web API deployment

5. IMPLEMENTATION

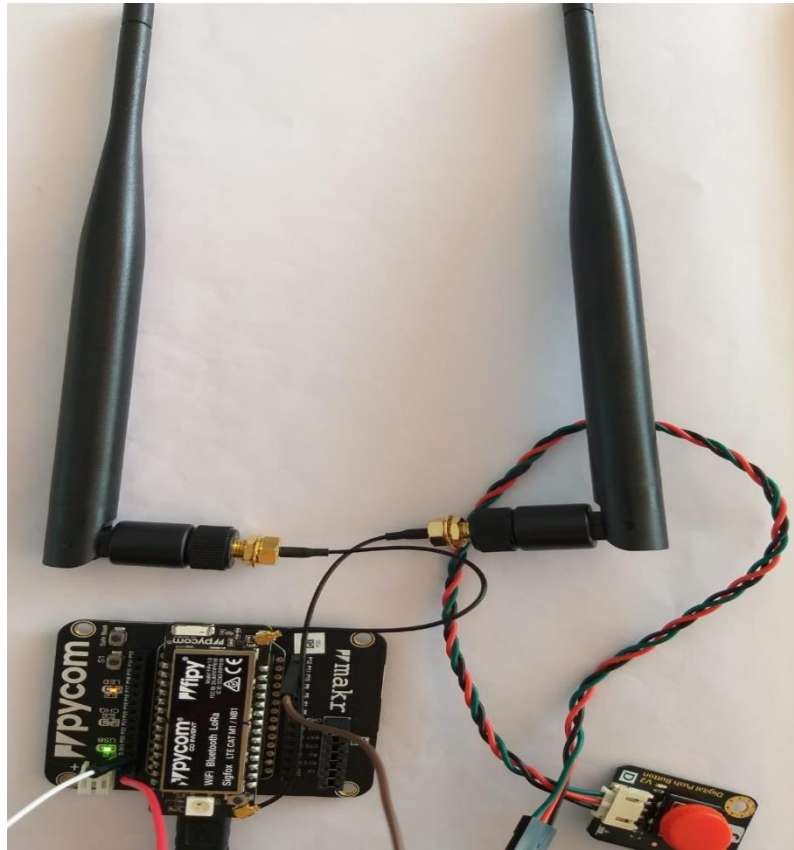


Fig 34: Implementation

5.1 BUTTON CLICK

Firstly, Pycom FiPy board is shielded on expansion board 3.1v and got powered up. Then the button is connected on PIN 12 when the push-button is not clicked, the input of the Pycom device is pulled to high (through an internal resistor which is enabled as Pull up). A Pin is one of the main module that used to control I/O operations (GPIO – General Purpose Input/ Output) when the button is pressed, the input is pulled to low. A push-button is connected to Fipy pin, and it has a wide voltage range from 3.3V to 5V. To enable the Pin function machine library will be imported.

5.2 BLUETOOTH

For connecting Bluetooth, Antenna has been connected to Pycom Fipy board; all these same antenna will be used for LoRa, Sigfox and Bluetooth. There is two antenna port on the FiPy board, the antenna port near the RGB led is for connecting Bluetooth antenna. After hardware connection, code has been done in Atom IDE, “import Bluetooth module from Network” has been done for importing the Bluetooth module and first, the FiPy (Safety Band) will advertise its name “SafetyBand” and UUID, if the client is connected to the Fipy board then the connection will be established to both the client and the board. Now, if the user clicks the button, then the trigger will be generated and sent to the client to which the Fipy board is connected.

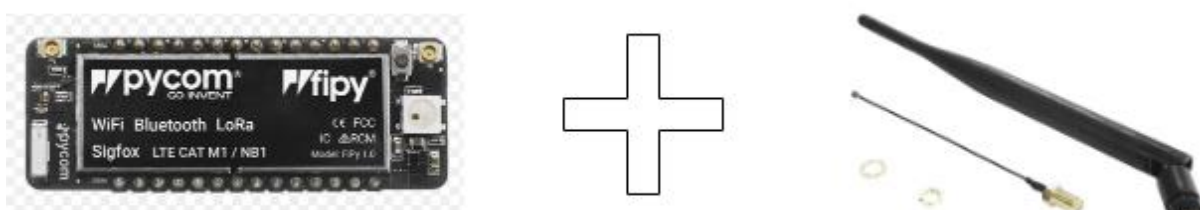


Fig 35: Bluetooth Implementation

5.3 MOBILE APPLICATION



Fig 36: Firebase cloud, Twilio, Android Integration

When the user turns ON the mobile application, Bluetooth/location service should be enabled. Pycom Bluetooth will be advertising its UUID, so once the user connects with the authenticated UUID the “Listener” function will be called and will be waiting for the trigger. There are four states for establishing the Bluetooth connection,

- Listening – waiting for the device connection.
- Connecting – Once the device is found, it will establish for the authentication connection.
- Connected – When the devices are connected
- Connection failed – If the connecting devices are unauthorized or Bluetooth service is not enabled in the mobile application.

```
//end of send recv

Handler handler = new Handler(new Handler.Callback() {
    @Override
    public boolean handleMessage(Message msg) {

        switch (msg.what) {
            case STATE_LISTENING:
                textViewBlueTooth.setText("Listening");
                break;
            case STATE_CONNECTING:
                textViewBlueTooth.setText("Connecting");
                break;
            case STATE_CONNECTED:
                textViewBlueTooth.setText("Connected");
                break;
            case STATE_CONNECTION_FAILED:
                textViewBlueTooth.setText("Connection Failed");
                break;
            case STATE_MESSAGE_RECEIVED://hit once data received
                byte[] readBuff = (byte[]) msg.obj;
                String tempMsg = new String(readBuff, 0, msg.arg1);
                // text.setText(tempMsg); <-- if I put this line the text will be elp
                if (tempMsg == "help") { //the handler check is the message is == to help
                    SendSms();
                }
                break;
        }
        return true;
    }
});

public void SendSms() {
    sendEmergencyText();
    runOnUiThread(new Runnable() {
```

Fig 37: Bluetooth Connection Establishing

Once, the device is connected, **the user** we will get a toast notification in the mobile application as well as the Bluetooth field in the mobile application will show “Connected”. Now the bluetooth_connect_function () will be waiting for a trigger (Button Click) to be received. Once the trigger is received to the mobile application via Bluetooth, mobile application backend will be running a small filtering algorithm. This filtering will be queried from the mobile application backend to the firebase real-time database API.


```

}
//filtering 8KM from firestore
private void sendSurroundText(FirebaseFirestore db, GeoPoint geoPoint) {
    double latitude = geoPoint.getLatitude();
    double longitude = geoPoint.getLongitude();
    int distance = 8; //8 miles
    GeoPoint lq = new GeoPoint(latitude, longitude);

    // -1 mile of lat and lon in degrees
    double lat = 0.0144927536231884;
    double lon = 0.01818181818182;

    final double lowerLat = latitude - (lat * distance);
    final double lowerLon = longitude - (lon * distance);
    double greaterLat = latitude + (lat * distance);
    final double greaterLon = longitude + (lon * distance);

    final GeoPoint lesserGeopoint = new GeoPoint(lowerLat, lowerLon);
    final GeoPoint greaterGeopoint = new GeoPoint(greaterLat, greaterLon);

    db.collection(collectionPath: "users").CollectionReference
        .whereGreaterThan(field: "currentlocation", lesserGeopoint) Query
        .whereLessThan(field: "currentlocation", greaterGeopoint) Query
        .get() Task<QuerySnapshot>
        .addOnCompleteListener(new OnCompleteListener<QuerySnapshot>() {
            @Override
            public void onComplete(@NonNull Task<QuerySnapshot> task) {
                if (task.isSuccessful()) {
                    for (QueryDocumentSnapshot document : task.getResult()) {
                        String number=document.getId();
                        String sms="Alert from safety band !. Someone need your help\n\n https://www.google.com/maps/search/?api=1&query="+geoPoint.getLa

                        sendEmergencySmsFromProvider(number,sms, geoPoint);
                    }
                }
            }
        });
}

```

Fig 38: Filtering Process in Android Back-end

5.3.1 FB Query:

Primary key: User Account Number

- User Current Location.
- User Emergency Contact Number.
- Other active devices which will be ≤ 8 KM (location and phone number).

The user account number will be the primary key, so it will take the current location of the users and the emergency contact numbers. Moreover, based on the user current user location, it will start filtering the active devices around 8 KM, after filtering all the active devices nearby, their primary mobile number has been taken and stored in the variable “number” (this will have both emergency contact number as well as the queried numbers).

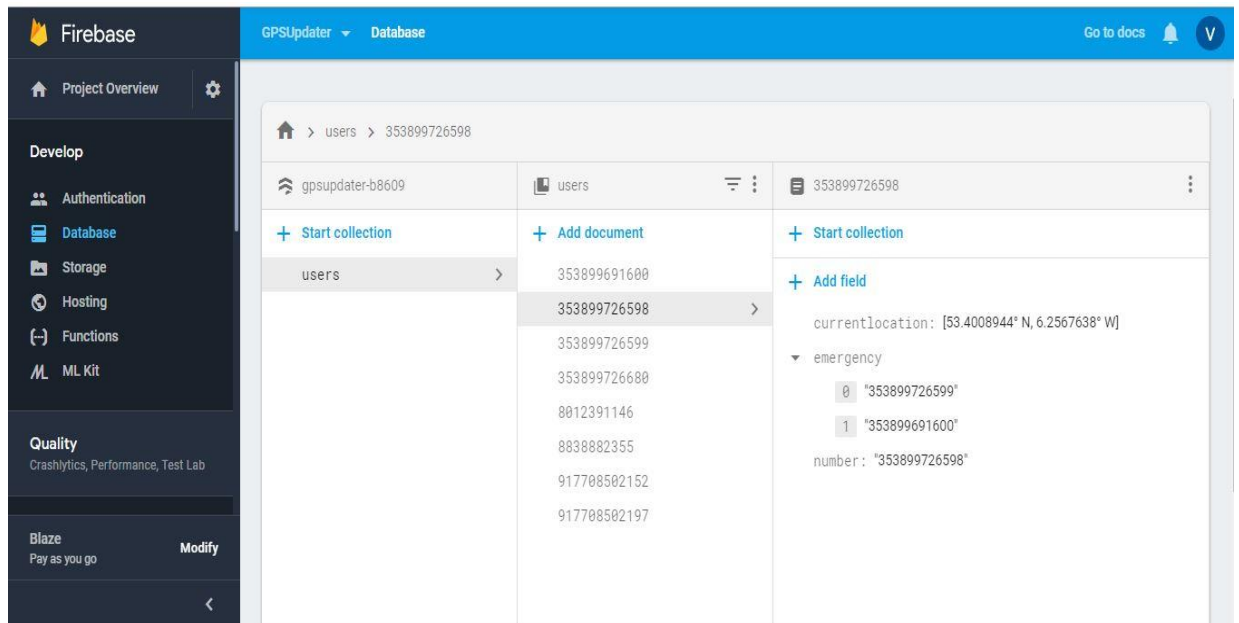


Fig 39: Firebase Database

If the trigger is updated in the database and filtering is done, the user will get “sucess” notification. Incase of network failure, if the data cannot reach the <https://gpsupdater-b8609.firebaseio.com/locationalert> URL which is deployed in hosting page, then the user will be getting “failed to send”.

```

// send sms to a number
private void sendEmergencySmsFromProvider(String number, String sms, GeoPoint geoPoint) {
    RequestQueue queue = Volley.newRequestQueue( context: MainActivity.this);
    String url = "https://gpsupdater-b8609.firebaseio.com/locationalert";
    StringRequest postRequest = new StringRequest(Request.Method.POST, url,
        new Response.Listener<String>() {
            @Override
            public void onResponse(String response) {
                Toast.makeText( context: MainActivity.this, text: "Success", Toast.LENGTH_SHORT).show();
            }
        },
        new Response.ErrorListener() {
            @Override
            public void onErrorResponse(VolleyError error) {
                Toast.makeText( context: MainActivity.this, text: "Failed to send", Toast.LENGTH_SHORT).show();
            }
        }
    );

    {
        @Override
        protected Map<String, String> getParams() {
            Map<String, String> params = new HashMap<>();
            params.put( key: "sms", sms);
            params.put( key: "number", number);
            params.put( key: "lat", value: ""+geoPoint.getLatitude());
            params.put( key: "lng", value: ""+geoPoint.getLongitude());
            // params.put("from", ""+geoPoint.getLongitude());
            return params;
        }
    };
    queue.add(postRequest);
}

```

Fig 40: URL Request

5.3.2 WEBAPI

The Queried data (User Current Location (Latitude and Longitude), User emergency contact number, and filtered near active device numbers) will be sent in the post method to the firebase WEB API which will be deployed in the hosting page. URL:

<https://gpsupdater-b8609.firebaseio.com/locationalert>

Firstly, the query parameter length will be checked, through post method the queried length will be four as it gets (Lat, Log, Queried numbers and SMS), if the length is less than 4, then it is the location data from Sigfox. All these data will be parsed and will bind to the Twilio SMS API. Using the Twilio Programmable API, the parsed data will be sent as a message to the numbers that are filtered with the victim's current location.

```
/* Twilio API Integration */
app.post('/locationalert',(req,res)=>{
  // fetching request parameter and store it into the value based on this variable we can process
  var sendmsgsftrprse = url.parse(req.url, true);

  if((Object.keys(req.query).length)>=4){
    // initializing the Twilio sms send api call
    client.notify.services(notifyServiceSid)
      .notifications.create({
        toBinding:JSON.stringify({
          binding_type : 'sms', address: sendmsgsftrprse.query.number
        }),
        body : sendmsgsftrprse.query.sms+" Latitude: "+sendmsgsftrprse.query.lat+" Longitude: "+sendmsgsftrprse.query.lng
      })
    // returning the sent notification id from twilio
    .then(notification=> res.send(notification.sid))
    .catch(error => res.send(error));
  }
```

Fig 41: Web API for mobile application

5.4 SIGFOX

Initially, the trigger will be generated to both the mobile application and Sigfox module. The Sigfox geo-location will be sent to the Sigfox backend, a custom call back will be created through, and the data will be sent through POST method to

[URL:https://gpsupdater-b8609.firebaseio.com/locationupdate](https://gpsupdater-b8609.firebaseio.com/locationupdate).

Device type PYCOM_DevKit_2 - Callback edition

Callbacks

Type: **SERVICE** | **DATA_ADVANCED**

The DATA ADVANCED callback is delivered with a delay of approximately 30 seconds.

Channel: **URL**

Custom payload config: [?](#)

URL syntax: `http://host/path?id={device}&time={time}&key1={var1}&key2={var2}...`
Available variables: `device, time, data, seqNumber, lqi, fixedLat, fixedLng, operatorName, countryCode`
Additional body variables: [?](#) `computedLocation`
Custom variables:

The feature send duplicate and the following information: `snr, station, avgSnr, lat, lng, rssi`, will not be available anyn 2019.

Url pattern: `https://gpsupdater-b8609.firebaseio.com/locationupdate`

Use HTTP Method: **POST**

Send SNI: ☒ (Server Name Indication) for SSL/TLS connections

Headers: header value

Content type: `application/json`

Body:

```
{
  "computedLocation": {computedLocation}
}
```

Fig 42: Sigfox Callback

As per Sigfox documentation, for Geo-location service, it is given that the Sigfox backend, will be filled in the entire object. There is no need to fill in the structure manually. The call back body is supposed to look like:

```
{
  "computedLocation": {computedLocation}
}
```

5.4.1 WEB API

The geo-location data that comes, from the Sigfox device, will have Latitude and Longitude (2 parameters). The request.query parameter has been checked if the length is ≥ 4 then the condition falls into the mobile application Twilio API or it will go into Sigfox Twilio SMS API, and this is because, for mobile application, the filtering algorithm was done in the Android backend. But for Sigfox (fall back) the filtering was done in Web API side.

```

} else {
  const cities = geo.collection('users')
  // setting up the geo point for db search based on band requested lat, long
  const center = geo.point(sendmsgsftrprse.query.lat, sendmsgsftrprse.query.lng);
  // setting up the searching radius we can extend the radius based on our requirement
  const radius = 8; // km

  const field = 'currentlocation';

  const query = cities.within(center, radius, field);

  // running loop for stored values in variable query
  query.forEach(filter_rec => {
    // initializing the Twilio sms send api call
    client.notify.services(notifyServiceSid)
      .notifications.create({
        toBinding: JSON.stringify({
          binding_type : 'sms', address: filter_rec.number
        }),
        body : "I'm In Emergency"+" Latitude: "+sendmsgsftrprse.query.lat+" Longitude: "+sendmsgsftrprse.query.lng
      })
      .then(notification=> res.send(notification.sid))
      .catch(error => res.send(error));
  });
}

```

Fig 43: Web API for sigfox

6. RESULTS

6.1 INSTALLING SAFETY BAND MOBILE APPLICATION

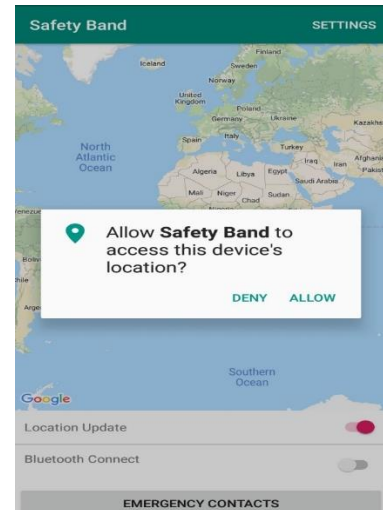
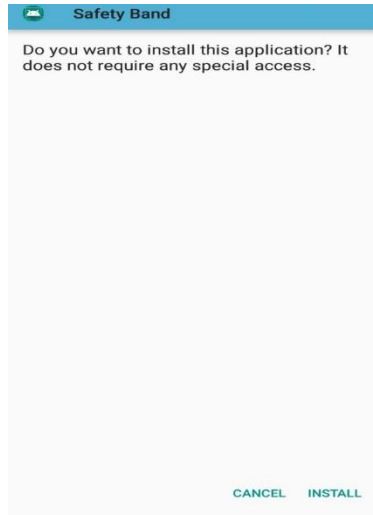


Fig 44: Installing Safety Band Mobile application. Fig 45: Location Access Enable

First, the user has to install the “Safety Band Mobile Application” to connect to the Fipy board (Safety Band). Next, to access the Location, user have to allow the app to use their location for tracking. Based on the GDPR rules, all the information that has been collected for this app will be only for the tracking process and will not be misused. Once the installation steps are completed, we have to setup an account for the user.

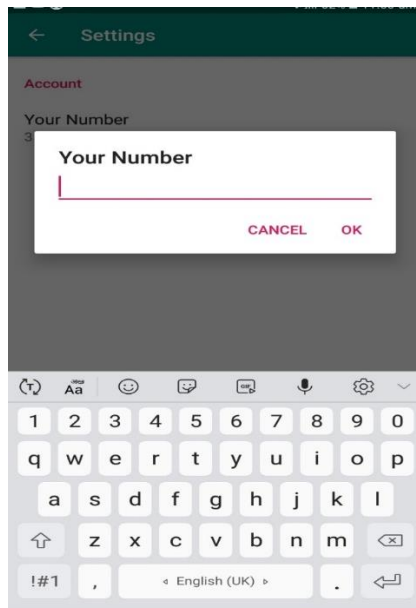


Fig 46: Adding Emergency contact

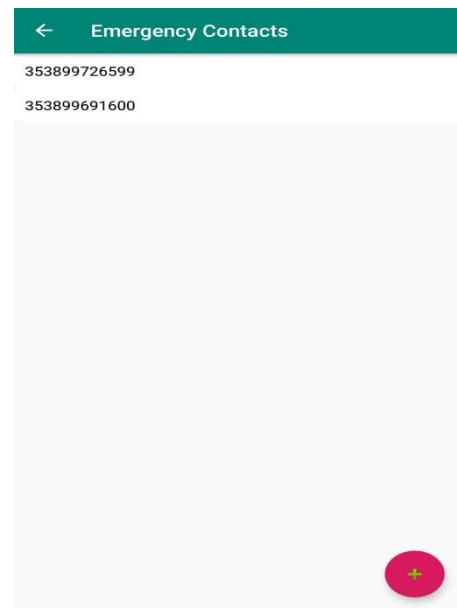


Fig 47: Display of Emergency Contact

Account setting is the important phase, in settings account number is added for the user, this will be the main primary key in the database. Then then emergency contact numbers can be added. A user can add multiple emergency contact number they want, if they are travelling to different places, they can also update according to that. Once all the basic set is done setup. Next, if the user wants to connect the band to the mobile application, then they have to turn on the location /Bluetooth services. In the bottom of the app there is an option to slide to turn on these services. Now, the Application is ready and will be waiting for the trigger to come and activate the process. If the button us clicked by the user, a trigger will be generated and will wake up the mobile application, all the fetching and filtering will be done in the Android Application backend. All the queried data will be sent to the hosting page, and the twilio SMS API will get all the data in POST method. So, finally, all the filtered numbers (active nearby users) and emergency numbers will get the alert SMS notification with the location of the victim.

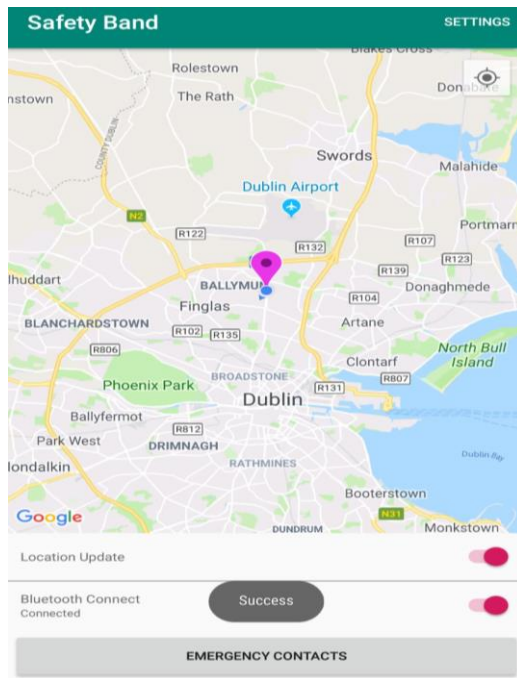


Fig 48: location Updated in Database

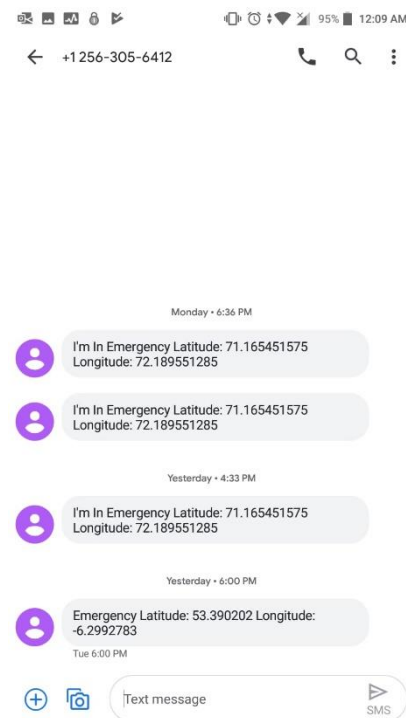


Fig 49: Message received to emergency contact



Fig 50: Message received to nearby devices

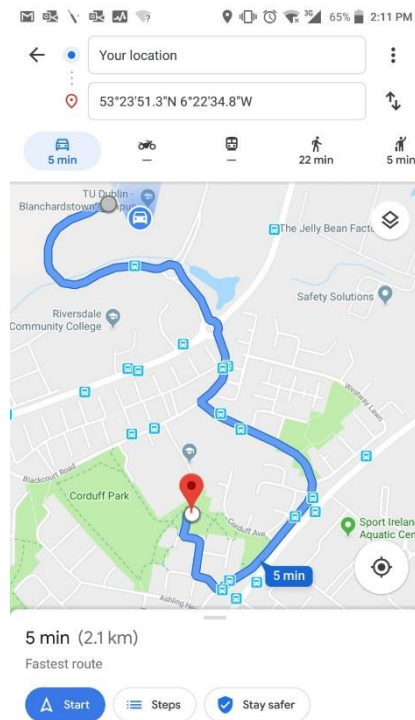


Fig 51: Location of Victim

6.2 LIMITATIONS

The aim of this thesis is to send SOS alert to the emergency contacts as well as to the near device available, this alert should reach the end user even though if there is no network Coverage. During the research, the one main problem was the Pycom discussion forum, it is not so active like other forums like Sigfox or Stack overflow. Additionally, Atom IDE which was used to code has many bugs and there was no proper updates on the packages. Especially, in Atom 1.39.1 has many bugs. When installing Pymakr plugin there was many issues. Additionally, the main limitation in this thesis was, the Sigfox module. The main aim is to send alert message to the near active device available, and the secondary important module is Sigfox. If there is no mobile network, then the near device will get alert notification through Sigfox. This research implemented on tracking

the precise location of the victim to protect women from the situation but the main problem arises is the Sigfox geo location is not so precis, as the sigfox geo-location is been calculated based on Sigfox LQI. Moreover some other features are stop from the sig-fox from June 2019.

7. CONCLUSION

Nowadays women facing lot of problem in all over the world. Moreover, now a day's many women are getting sexually or mentally assaulted. To prevent this kind of cases the victim needs a proper communication to inform the close ones on the situation for help. But if the women is far away from their home, even if they need any help it is impossible for their family members to come and help them. The aim of this thesis is to help the women in her critical situation, this will act as a normal band with extra ordinary features. The primary research question of this research achieved successfully. The research question of the thesis is to send SMS alert to the nearby devices. On the other hand, the secondary research question cannot be achieved, the reason for this is Sigfox geo-location send approx. latitude and longitude data. Moreover, the Sigfox call back for geo-location is not subscribed in Pycom board. However, the backend filtrating algorithm has been done successfully. The web API deployment for Mobile side trigger and Sigfox is written successfully. In nutshell, the primary research question and objectives have been achieved successfully.

7.1 FUTURE WORK

In Future work, there will be upgradation of the band design and some modules will be added to trigger the event, Using Machine Learning algorithm, the emergency situation can be predicted and triggered. This can be done by monitoring the user behaviour and his daily routine, data can be collected and the machine will learn from his daily activities. Moreover, push button will be replaced with screaming sensor and motion sensor. Using Machine learning algorithm, the dataset will be trained the difference between normal human sound and scream during emergency as well as the normal movement and abnormal sudden motions will be captured and trained. Before triggering an even both the parameter the panic alert notifications will be send. Based on the user facial expression, the panic mode will be turned on with the live video recording. Moreover, the near device communication can be done using NB-IoT, the most advanced LPWAN.

BIBLIOGRAPHY:

A. Jatti, M. Kannan, R. M. Alisha, P. Vijayalakshmi & S. Sinha 2016, Design and development of an IOT based wearable device for the safety and security of women and girl children.

Adroher, A. (2015). *The Story of Pycom Things - Pycom*. [online] Pycom. Available at: <https://pycom.io/the-story-of-pycom-things/> [Accessed 5 Sep. 2019].

A. USHA KIRAN REDDY, P. SUSHMITHA, I. GAYATHRI, K. SANDHYA & N. SURESH 12345.

Ahamed, J. & Rajan, A.V. (Dec 2016) Internet of Things (IoT): Application Systems and Security Vulnerabilities. : IEEE, pp. 1.

Alleman, P., Poulton, C., Ismail, Y. and Gustiana, R. (2018). 16 actions for girls' and women's safety in emergencies - UNICEF Connect. [online] UNICEF Connect. Available at: <https://blogs.unicef.org/blog/16-actions-girls-womens-safety-emergencies/> [Accessed 28 Aug. 2019].

Alonso, L., Barbarán, J., Chen, J., Díaz, M., Llopis, L. & Rubio, B. (2018) Middleware and Communication Technologies for Structural Health Monitoring of Critical Infrastructures: A Survey. *Computer Standards & Interfaces*. 56 pp. 83-100.

Al-Sarawi, S., Anbar, M., Alieyan, K. & Alzubaidi, M. (May 2017) Internet of Things (IoT) Communication Protocols: Review. : IEEE, pp. 685.

Arthur, J. (2019) *Arduino*. La Vergne: Ingram Publishing.

Baichtal, J. (2013) *Arduino for Beginners* [online]. Available from: <http://proquest.tech.safaribooksonline.de/9780133416725> .

Balakrishnan, A. & Patapati, S. (Oct 2017) Automation of Traumatic Brain Injury Diagnosis through an IoT-Based Embedded Systems Framework. : IEEE, pp. 645.

Chan, M., Estève, D., Fourniols, J., Escriba, C. & Campo, E. 2012, *Smart wearable systems: Current status and future challenges*.

Chi-Yu You, Yan-Ling Hwang, Chuan-Kai Kao, Fu-Hau Hsu & Chia-Hao Lee (Jan 1, 2017) A Light-Weight Method to Send and Receive SMS Messages in an Emulator. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), pp. 197.

Condon, D. (2019). Violence against women in Ireland. [online] Irishhealth.com. Available at: <http://www.irishhealth.com/article.html?id=7787> [Accessed 28 Aug. 2019].

Cosc.ie. (2019). *Cosc, the National Office for the Prevention of Domestic, Sexual and Gender-based Violence: European Study Agency for Fundamental Rights (FRA) Report Violence Against Women Across the EU: Abuse at home, Work, in public and online.* [online] Available at: <http://www.cosc.ie/en/COSC/Pages/RD14000006> [Accessed 28 Aug. 2019].

Crucius, S. (2018). *Wearable Tech is Here to Stay with a Robust Presence in the Future Healthcare Industry.* [online] Wearable Technologies. Available at: <https://www.wearable-technologies.com/2018/06/wearable-tech-is-here-to-stay-with-a-robust-presence-in-the-future-healthcare-industry/> [Accessed 1 Sep. 2019].

D. Seth, A. Chowdhury & S. Ghosh 2018, A Hidden Markov Model and Internet of Things Hybrid Based Smart Women Safety Device.

Daniel Clement, Kush Trivedi & Saloni Agarwal Shikha Singh 2016, *AVR Microcontroller Based Wearable Jacket for Women Safety.*

Din, S. and Paul, A. 2019, *Smart health monitoring and management system: Toward autonomous wearable sensing for Internet of Things using big data analytics.*

Dorsemaine, B., Gaulier, J., Wary, J., Kheir, N. & Urien, P. (Sep 2015) Internet of Things: A Definition & Taxonomy. : IEEE, pp. 72.

Elena-Lenz, C. (2014). *Internet of Things: Six Key Characteristics - frog.* [online] frog. Available at: <https://designmind.frogdesign.com/2014/08/internet-things-six-key-characteristics/> [Accessed 9 Sep. 2019].

Enefiok, E. and Uzochukwu, O. (2016). An Android based Employee Tracking System. International Journal of Computer Applications, 153(3), pp.26-32.

Energy *MultihDoaptaTransfServifcoeBrluetooLtohw.*

Fernández-Garcia, R. & Gil, I. (2017) An Alternative Wearable Tracking System Based on a Low-Power Wide-Area Network. *Sensors (Basel, Switzerland)*. 17 (3), pp. 592.

Fra.europa.eu. (2014). [online] Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf [Accessed 25 Aug. 2019].

G, S., B. SELVA, K., R. PUSHPA, R. & R, P. (2016) Smart Safety Device for Security of Women. *I-Manager's Journal on Embedded Systems*. 5 (2), pp. 1.

Ghanchi, J. (2018). The Rapid Evolution Of IoT: Trends Shaping The Digital Landscape. [online] SmartData Collective. Available at: <https://www.smartdatacollective.com/rapid-evolution-iot-trends-shaping-digital-landscape/> [Accessed 20 Aug. 2019].

Gomez, C., Oller, J. & Paradells, J. (2012) Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors*. 12 (9), pp. 11734-11753.

Haney. (2013) *Independent project (degree project), 15 credits, for the degree of Bachelor of Science in Engineering Spring Semester 2018 Faculty of Natural Science*.

Harvey, C. (2017). [online] Available at: <https://www.datamation.com/cloud-computing/ibm-cloud.html> [Accessed 4 Sep. 2019].

Hossain, M.S. and Muhammad, G. 2016, *Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring*.

Jacobsen, R.H., Aliu, D. & Ebeid, E.S.M. 2017, *A Low-cost Vehicle Tracking Platform using Secure SMS*, SCITEPRESS Digital Library.

Joris, L., Dupont, F., Laurent, P., Bellier, P., Stoukatch, S. & Redoute, J. (2019) An Autonomous Sigfox Wireless Sensor Node for Environmental Monitoring. *IEEE Sensors Letters*. 3 (7), pp. 1.

Junger, M 1987, 'Women's experiences of sexual harassment: some implications for their fear of crime' *British journal of criminology*, vol. 27, no. 4, pp. 358-383.

Kammer, D. (2002) *Bluetooth*. Rockland, Mass: Syngress Publ.

Khan, R., Khan, S.U., Zaheer, R. & Khan, S. (Dec 2012) Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. : IEEE, pp. 257.

Klaus-Peter (2019) Schlotter kps@de.ibm.com *IBM Cloud Overview IBM Cloud Overview*.

Kokkinos, P., Varvarigou, T.A., Kretsis, A., Soumplis, P. & Varvarigos, E.A. (Jun 2013) Cost and Utilization Optimization of Amazon EC2 Instances. : IEEE, pp. 518.

Koss, M.P., Figueredo, A.J., Bell, I., Tharan, M. & Tromp, S. (1996) Traumatic Memory Characteristics: A Cross-Validated Mediation Model of Response to Rape among Employed Women. *Journal of Abnormal Psychology*. 105 (3), pp. 421-432.

Krco, S., Pokric, B. & Carrez, F. (Mar 2014) Designing IoT Architecture(s): A European Perspective. : IEEE, pp. 79.

Lamey, D. (2018). Past, Present and Future: The Evolution of Technology. [online] Discovertec.com. Available at: <https://www.discovertec.com/blog/evolution-of-technology> [Accessed 20 Aug. 2019].

Leu, F., Ko, C., You, I., Choo, K.R. & Ho, C. 2018, *A smartphone-based wearable sensors for monitoring real-time physiological data*.

Lightning talk and Hatim.Shahzada@assaabloy.com *Introduction to Bluetooth Low Energy*.

Madhur Bhargava (2017) *IoT Projects with Bluetooth Low Energy*. 1 ed. GB: Packt Publishing.

Mark R Murphy 2018, *Twilio*, JPMorgan Chase & Company, New York.

Mekki, K., Bajic, E., Chaxel, F. & Meyer, F. (2019) A Comparative Study of LPWAN Technologies for Large-Scale IoT Deployment. *ICT Express*. 5 (1), pp. 1-7.

Mwakwata, C.B., Malik, H., Alam, M.M., Moullec, Y.L., Parand, S. & Mumtaz, S. (2019) Narrowband Internet of Things (NB-IoT): From Physical (PHY) and Media Access Control (MAC) Layers Perspectives. *Sensors (Basel, Switzerland)*. 19 (11), pp. 2613.

Nandhini, P & Moorthi, K. (2018). A STUDY ON WEARABLE DEVICES FOR THE SAFETY AND SECURITY OF A GIRL CHILD AND WOMEN. *International Journal of Advanced Research*. 6. 231-237. 10.21474/IJAR01/7804.

National Sexual Violence Resource Center. (2019). Daily News Summary. [online] Available at: <https://www.nsvrc.org/news/daily-news-summary> [Accessed 25 May

2019].

O'donovan, A., Devilly, G.J. & Rapee, R.M. (2007) Antecedents to Women's Fear of Rape. *Behaviour Change*. 24 (3), pp. 135-145.

Patel, D.M. (2011) *Preventing Violence Against Women and Children* [online].

Patel, J. & Hasan, R. (Jan 2018) Smart Bracelets: Towards Automating Personal Safety using Wearable Smart Jewelry. : IEEE, pp. 1.

Patel, K. & Bhatt, N. (2019) IoT Enabled Wearable Camera for Emerging Application World. *International Journal of Advanced Networking Applications*. 10 (6), pp. 4090-4093.

Petajajarvi, J., Mikhaylov, K., Hamalainen, M. & Inatti, J. (Mar 2016) Evaluation of LoRa LPWAN Technology for Remote Health and Wellbeing Monitoring. : IEEE, pp. 1.

Prashanth, D.S., Patel, G. & Bharathi, B. (Apr 2017) Research and Development of a Mobile Based Women Safety Application with Real-Time Database and Data-Stream Network. : IEEE, pp. 1.

Rachana B. Pawar, Manali H. Kulabkar & Kirti S. Pawar Akshata R. Tambe Prof. Smita Khairnar 2018, *Smart Shield for Women Safety*.

Raffaele Stifani *IBM Bluemix*.

Rai, U., Miglani, K., Saha, A., Sahoo, B. & Vergin Raja Sarobin, M. (Nov 2018) ReachOut Smart Safety Device. : IEEE, pp. 131.

Ramnatthan Alagappan *Uncovering Twilio: Insights into Cloud Communication Services*.

RANDALL, M. and HASKELL, L. (1995) 'Sexual Violence in Women's Lives: Findings from the Women's Safety Project, a Community-Based Survey', *Violence Against Women*, 1(1), pp. 6–31.

Ray, B. (2017). *What is Narrowband IoT (NB-IoT)? - Explanation and 5 Business Benefits*. [online] IoT For All. Available at: <https://www.iotforall.com/what-is-narrowband-iot/> [Accessed 2 Sep. 2019].

Rouse, M. (2017). What is Amazon S3 bucket? - Definition from WhatIs.com. [online] Search AWS. Available at: <https://searchaws.techtarget.com/definition/AWS-bucket> [Accessed 3 Sep. 2019].

Samsung Semiconductors India, R. and D Centre *Sreelakshmi Gollapudi, Lalit Kumar Pathak, Tushar Vrind, Diwakar Sharma, Samir Kumar Mishra.*

Seth, D., Chowdhury, A. & Ghosh, S. (Jun 2018) A Hidden Markov Model and Internet of Things Hybrid Based Smart Women Safety Device. : IEEE, pp. 1.

Shilpa, B. & Mahamood, M.R. (2017) Design and Implementation of Framework for Smart City using Lora Technology. *SREYAS International Journal of Scientists and Technocrats*. 1 (11), pp. 36-43.

SÖChting, I., Fairbrother, N. & Koch, W.J. (2004) Sexual Assault of Women. *Violence Against Women*. 10 (1), pp. 73-93.

Sogi, N.R., Chatterjee, P., Nethra, U. & Suma, V. (Jul 2018) SMARISA: A Raspberry Pi Based Smart Ring for Women Safety using IoT. : IEEE, pp. 451.

Swain, G. (2001) *Celebrating*. Nachdr. ed. Minneapolis: Carolrhoda Books.

The Indian Express. (2019). National Crime Records Bureau data, 2015: Slight dip in rape, crime against women. [online] Available at: <https://indianexpress.com/article/explained/national-crime-records-bureau-data-2015-slight-dip-in-rape-crime-against-women-3004980/> [Accessed 28 Apr. 2019].

The Indian express. (2019). national crime records bureau data, 2015: slight dip in rape, crime against women. [online] available at: <https://indianexpress.com/article/explained/national-crime-records-bureau-data-2015-slight-dip-in-rape-crime-against-women-3004980/> [accessed 28 apr. 2019].

Tripathy, Bk;anuradha & J (2017) *Internet of Things (IoT)*. 1 ed. Milton: CRC Press.

Tripti, N.F., Farhad, A., Iqbal, W. & Zaman, H.U. (Aug 2018) SaveMe: A Crime Deterrent Personal Safety Android App with a Bluetooth Connected Hardware Switch. : IEEE, pp. 23.

Tudip. (2019). *Comparing IoT Services: AWS vs Azure vs Google vs IBM / Tudip*. [online] Available at: <https://tudip.com/blog-post/comparing-iot-services-with-aws-vs-azure-vs-google-vs-ibm/> [Accessed 4 Sep. 2019].

UKEssays. November 2018. How to Write a Masters Dissertation Literature Review. [online]. Available from <https://www.ukessays.com/resources/masters/how-to-write-a-masters-dissertation-literature-review.php?vref=1> [Accessed 28 August 2019].

UN Women. (2019). *UN Women - United Nations Entity for Gender Equality and the Empowerment of Women*. [online] Available at: <https://www.unwomen.org/en> [Accessed 28 Aug. 2019].

Vejlgaard, B., Lauridsen, M., Huan Nguyen, Kovacs, I.Z., Mogensen, P. & Sorensen, M. (Jun 2017) Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT. : IEEE, pp. 1.

Viswanath, N., Pakyala, N.V. & Muneeswari, G. (May 2016) Smart Foot Device for Women Safety. : IEEE, pp. 130.

Wade, J. (2017). Wearable Technology statistics and trends 2018 | Smart Insights. [online] Smart Insights. Available at: <https://www.smartinsights.com/digital-marketing-strategy/wearables-statistics-2017/> [Accessed 28 Aug. 2019].

Wearable device for the Safety and Security of 2016, *Design and Development of an IOT based*.

Who.int. (2019). Violence against women. [online] Available at: <https://www.who.int/news-room/fact-sheets/detail/violence-against-women> [Accessed 25 Aug. 2019].

Yeonjoon Chung, Jae Young Ahn, Jae Du Huh Hyper-connected Basic Technology Research Division, Hyper-connected Communication Research Laboratory, Electronics, Telecommunications Research Institute Deajeon, Korea (ychung, ahnjy & jdjuh, 2018) *Experiments of A LPWAN Tracking(TR) Platform Based on Sigfox Test Network*.

APPENDIX A

```
bluetooth.py
from network import Bluetooth

bluetooth = Bluetooth()
bluetooth.set_advertisement(name='SafetyBand', service_uuid=b'0600010f2002493c8124925aae617c9d30f482870267f38fe407c3f7ee')

def conn_cb (bt_o):
    events = bt_o.events() # Here we are checking if a device is connected.
    if events & Bluetooth.CLIENT_CONNECTED:
        print("Client connected")
    elif events & Bluetooth.CLIENT_DISCONNECTED:
        print("Client disconnected")

bluetooth.callback(trigger=Bluetooth.CLIENT_CONNECTED |
Bluetooth.CLIENT_DISCONNECTED, handler=conn_cb)
```

Fig 52: Bluetooth advertising to connect with client

```
JS index.js x
1 const functions = require('firebase-functions');
2 const firebase = require('firebase-admin');
3 const express = require('express');
4 const engines = require('consolidate');
5 var serviceAccount = require("../gpsupdater-b8609-firebase-adminsdk-52qxj-dde6a13c98.json");
6 var bodyParser = require('body-parser')
7 const firebaseAdmin = firebase.initializeApp({
8     credential: firebase.credential.cert(serviceAccount),
9     databaseURL: "https://gpsupdater-b8609.firebaseio.com"
10 });
11
12 let db = firebaseAdmin.firestore();
13
14 const accountSid = 'AC7fe7564daa6b5cdc7092b0ffdb4d8a04';
15 const authToken = '96e1b154826cbd25e48ea104b57ad698';
16 const notifyServiceSid = 'ISba525917f121e1f88607a3e315deaefe';
17
18 const client = require('twilio')(accountSid, authToken);
19
```

Fig 53: Twilio API Credentials

APPENDIX B

GitHub Link:

<https://github.com/vigneswaranjaga/finalthesis>

