IOT BASED PERSONAL SAFETY AND PROTECTION SYSTEM

LIAU KAI HAO

A project report submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering (Honours) Mechatronics Engineering

Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

Jan 2021

DECLARATION

I hereby declare that this project report is based on my original work except for citations and quotations which have been duly acknowledged. I also declare that it has not been previously and concurrently submitted for any other degree or award at UTAR or other institutions.

Signature : 

Name : LIAU KAI HAO

ID No. : 16UEB03412

Date : 5/5/2021

APPROVAL FOR SUBMISSION

I certify that this project report entitled **"IOT BASED PERSONAL SAFETY AND PROTECTION SYSTEM"** was prepared by **LIAU KAI HAO** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Engineering (Honours) Mechatronics Engineering at Universiti Tunku Abdul Rahman.

Approved by,

Signature : 

Supervisor : MR. CHAI TONG YUEN

Date : 5/5/2021

ACKNOWLEDGEMENTS

I would like to thank everyone who had contributed to the successful completion of this project. I would like to express my gratitude to my research supervisor, Mr. Chai Tong Yuen for his invaluable advice, guidance, and his enormous patience throughout the development of the research.

In addition, I would also like to express my gratitude to my loving parents and friends who had helped and given me encouragement throughout the entire process.

ABSTRACT

As urbanisation becomes more rapid, the problem of poverty has become more serious, and the poor can only try to harm others to get money for living. To guarantee the safety of an individual, the Internet of Things (IoT) based personal security or protection systems are introduced. However, the conventional systems do not offer a constant performance, in which their triggering methods are too simple and impractical in the real world. They have no measure on false alarm prevention, causing unstable performance of the systems. In this project, IoT technology is applied to develop a more reliable personal safety and protection system that can automatically respond against dangerous situations with three activation methods that avoid false alarms and store the data in the Firebase database. There are four major parts in the proposed system, which are sensing, processing, actuating, and visualising units. The sensing unit is an integration of sensors and receivers that receives input continuously, while the actuating unit is a combination of actuators that carry out response towards an emergency. Besides, the processing unit is a Raspberry Pi, while the visualising unit is an Android application that communicates with the Firebase database. Real-time monitoring and controlling of the system are achieved by the communication between the Firebase real-time database and Android application. Experiments are conducted on the proposed system, and the results have proved its functionality, accuracy, and precision.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS / ABBREVIATIONS

CCTV	closed-circuit television
IoT	Internet of Things
USB	Universal Serial Bus
IMU	Inertial Measurement Unit
TTL	Transistor-transistor Logic
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IDE	integrated development environment
ASR	automatic speech recognition
FFT	fast Fourier transform
HMM	Hidden Markov Model
API	Application Programming Interface
Wi-Fi	Wireless Fidelity
LAN	local area network
3G	Third Generation
WWANs	Wireless Wide Area Networks
WMANs	Wireless Metropolitan Area Networks
WLANs	Wireless Local Area Networks
WPANs	Wireless Personal Area Networks
UWB	Ultra-Wideband
WiMAX	Worldwide Interoperability for Microwave Access
UMTS	Universal Mobile Telecommunication System
GPRS	General Packet Radio Service
GUI	graphical user interface
OS	operating system
UART	Universal Asynchronous Receiver/Transmitter
GPIO	general-purpose input/output
IC	integrated circuit
EEPROM	electrically erasable programmable read-only memory
SMS	short message service
SDKs	Realtime Database Software Development Kits
SSH	Secure Shell

XML	Extensible Markup Language
PCB	printed circuit board
RX	receive
TX	transmit
JSON	JavaScript Object Notation
APK	Android application package
SI	International System of Units
SIM	subscriber identification module

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 General Introduction

A security or protection system is a combination of various single products to build a complete closed-loop system that aims to keep people safe and protected. According to American District Telegraph (ADT) (n.d.), the world's first residential security system network was invented in 1874 by its founder, Edward Callahan. This was a telegraph-based “call-box” that can convey signals for assistance to a central office. About 50 homes took part in the testing of this residential security system by connecting to the system within the neighbourhood, making it a success.

The ancient security system can be said to exist even longer before the innovation of the first residential security system. Our bright ancestors had done a few important creations that are still being used currently as basics to stack up the modern security system. A watchtower is the most significant security system in the old time. During this time, watchtowers were built in major cities for the purpose to keep an eye on who is coming and going. They were mostly found near prisons and top-secret government facilities. The working concept of a watchtower is critically identical to closed-circuit television (CCTV) or better known as a surveillance camera that is widely used nowadays. Monitoring of the condition in a location can be done on watchtowers in the ancient or through surveillance cameras at present to take full advantage of remote viewing and live feeds. Another great innovation of the ancient security system was the gates. During the warring states period in China, huge gates were used as the borders to control the movement of people in and out of every city. Today, gates have become more attractive in colour and design, and are used as decorations. However, gates still provide essential protection to the people inside a house.

As urbanisation becomes more rapid, someone is left behind. Normally, the poor are abandoned in the development plan because they cannot help with anything. Over the time, the problem of poverty has become more serious and the poor can only try to steal, rob, and harm others to get money for living.

Furthermore, mental problems are becoming more common in the community due to over-stressed under the fast pace of development that brings higher living costs. A patient suffering from mental problems may try to harm a victim unconsciously as he cannot control himself. Thus, a personal security or protection system is important to guarantee the safety of an individual. A conventional personal protection system is usually used as a weapon for self-defence, like the stun gun and pepper spray. This can only help the victim to get rid of the dangerous situation for a short moment and no one will notice that he is getting harmed. Therefore, there is an emerging trend of utilising the Internet of Things (IoT) based personal protection system to supplant the conventional personal protection system.

In recent years, many researchers have developed various types of IoT based personal safety and protection systems. The working principles of these systems are almost identical, where a central processing unit, such as a microcontroller or microprocessor is used to control a series of sensors, obtain the data from the sensors, process the data collected, and implement proper actions as the feedback. During these processes, the information obtained will be uploaded and stored in a cloud server to prepare for data analysis or visualisation. The IoT acts as a communication platform that links all the sensors and devices in a single network to allow the transmission of data in a very short time. Real-time monitoring is one of the useful functions provided by IoT technology to provide real-time support when the user is in danger.

This study is to design and develop a system that is capable of protecting the user when facing some risks. Two sensors, a receiver, an actuator (buzzer), and two communication modules are used in the system. All the data collected will be uploaded to the cloud server continuously, and actions will be generated when it detects unusual data from the sensors. A detailed description of the system will be elaborated in Chapter 3.

1.2 Importance of the Study

From Figure 1.1, although the crime index ratio per 100000 population for Malaysia in 2018 had improved to 273.8 as compared to 309.7 in 2017, seven states were still recorded the crime index above the national level, namely Johor (275.7), Penang (284.6), Kedah (287.6), Malacca (303.6), Negeri Sembilan (327.1), Selangor (330.8), and W.P. Kuala Lumpur (642.6). These are the major cities in Malaysia, where they are home to more than half of the total residents in the country. It is expected that crime cases per year will still maintain at an unhealthy level in the near future. In 2018, there were about 90000 crime cases throughout the nation, of which 19% were violent crimes and 81% were property crimes. 60.8% of violent crimes were robbery, which is very common to happen in Malaysia when an individual is alone. Therefore, it is important to develop a more reliable personal safety and protection system that will be able to reduce the crime rate, not only in Malaysia but throughout the world. With the help of advanced technology like the IoT, the personal safety level can be increased. This study may contribute to a better living environment with lesser crime cases and a higher public safety level.

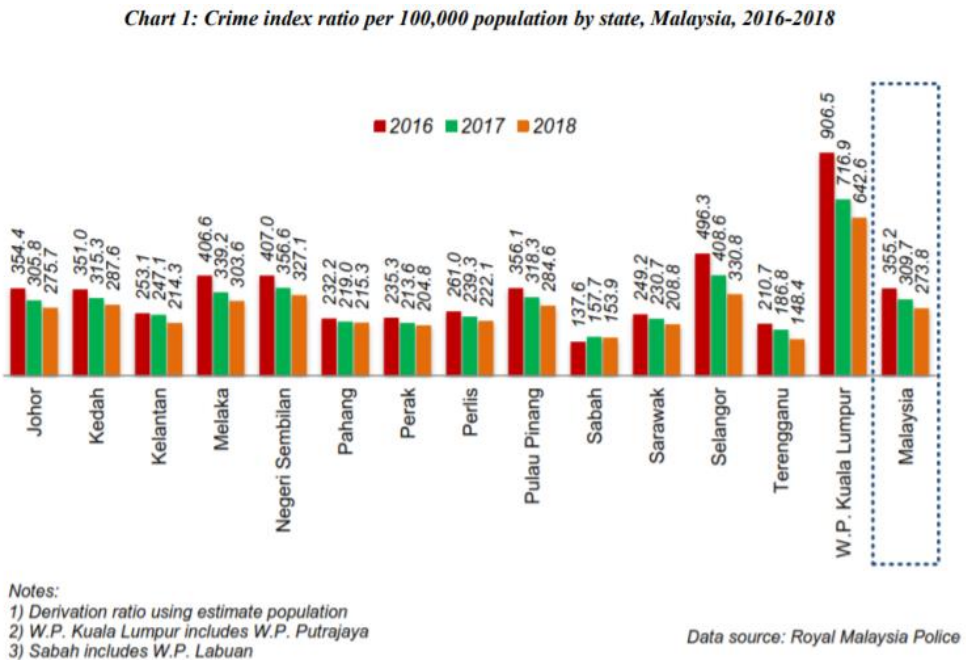


Figure 1.1: Statistics of crime index ratio in Malaysia (Department of Statistics, Malaysia, 2019).

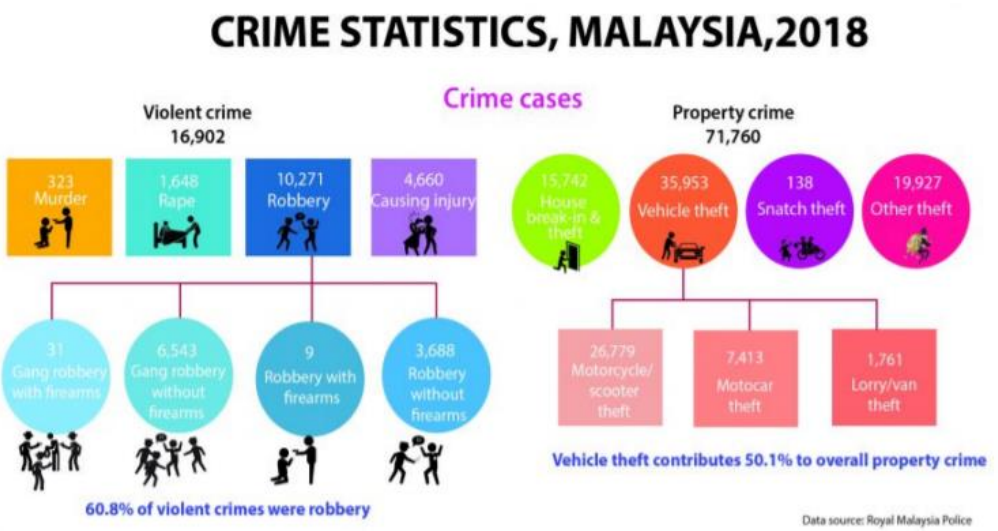


Figure 1.2: Cumulative number of crime cases in Malaysia in 2018 (Department of Statistics, Malaysia, 2019).

1.3 Problem Statement

A typical personal safety and protection system consists of various sensors and actuators connected to the central control panel using wires. Whereas, a conventional IoT based personal safety and protection system establishes a communication network to link and control the actions and operations of the system automatically and remotely.

There are some limitations to previous literature done by other researchers. Firstly, the user must have direct contact with the existing devices in order to trigger the system. For example, in the project developed by Vijaylashmi, et al. (2015), a physical press on the mechanical button must be carried out to activate the protection system. This is the only way to start up the system, which may be unreliable as the user has to take out the device from his pocket or bag and search for the position of the button under an emergency condition. There is a high possibility that the protection system fails to be activated and victimisation will happen.

Furthermore, the existing personal protection system is not equipped with a false alarm prevention system. A false alarm can be easily initialised when the system possesses too simple triggering methods. The user may push on the physical button accidentally without his notice. This problem has affected the accuracy and reliability of the system. For example, in the project constructed by Ahir, et al. (2018), only a double-tap on the device's screen is

necessary to activate the system. Thus, an unintentional activation may occur without prior notice from the user. A false alarm will cause the emergency contacts of the user to always live in fear and result in the wastage of public resources, such as the police force.

Next, some of the existing systems do not come with a user interface. The user cannot have real-time monitoring of the protection system, in which he does not know whether the system is running. This makes the sense of security of the user to be very weak. Also, no customisation and tuning are available for the user as the existing systems only come with a single device. This may be not user-friendly to suit the requirement of the user. By developing an Android application as the user interface, the user can simply monitor, control, and alter whatever features according to his need.

1.4 Aim and Objectives

The main aim of this project is to develop a reliable personal safety and protection system through IoT technology. The achievement of the aim will overcome most of the limitations in the current research, where a more precise and dependable system will be produced. The specific objectives required to be fulfilled in achieving the aim are:

(i) To design and develop a reliable system, which is able to protect and support the user during an emergency as well as store data on cloud storage.

(ii) To avoid false alarm.

(iii) To develop an Android application to display real-time data and perform real-time control.

1.5 Scope and Limitation of the Study

The scope of this project is to focus on developing an IoT based personal safety and protection system. The prototype consists of a sensing unit, a processing unit, an actuating unit, and a visualising unit. Apart from the prototype, an Android application will be developed to work closely with the system. A combination of hardware and software will be involved in the development of the proposed system:

(i) Hardware: Raspberry Pi 3 Model B+, TTP223 Capacitive Touch Sensor, Universal Serial Bus (USB) microphone, buzzer, MPU9250 9-axis Inertial Measurement Unit (IMU) Sensor, CH340G USB to Transistor-transistor Logic (TTL) Converter Module, GY-NEO6MV2 Global Positioning System (GPS) Tracking Module, and SIM800L Global System for Mobile Communications (GSM) Module.

(ii) Software: Firebase Cloud Server, Visual Studio Code, Android Studio IDE, and Fritzing.

The first limitation of this project is the size of the prototype. The prototype developed will be too big for convenient usage. This is due to the budget constraint, where an integrated circuit design is not able to be done. All the hardware is bought and installed separately that makes the prototype large and heavy. Next, the cloud server only permits storage of 20000 data per day for the free version. If the system developed is going to be used for 24 hours per day, there will be insufficient data storage, leading to failure of the entire system. Since this is a conceptual design, all these limitations can actually be overcome when this prototype is put into mass production.

1.6 Contribution of the Study

In this project, a new concept of personal safety and protection system based on the Internet of Things approach is discussed. The main contributions are as follow:

(i) Review the existing personal safety and protection system.

(ii) Identify the problems and challenges of the conventional personal safety and protection system.

(iii) Implement the Firebase real-time database to store data from sensors.

(iv) Develop an Android application that acts as the graphical user interface for real-time monitoring and controlling.

(v) Read and write data on the Firebase real-time database to build the communication between the safety device and the Android application.

(vi) Produce a functional prototype and all details are recorded to act as the reference for future research, improvement, and development.

1.7 Outline of the Report

This report consists of five chapters. The first chapter introduces the old and new security and protection systems and their significance to be enhanced, the problems faced by the current personal protection system, aim and objectives to solve the problems, scope and limitation of the study, and contribution of the study. Chapter 2 reviews multiple related pieces of literature to discover the theories and concepts required in accomplishing this project. In the third chapter, the methodology of the project is discussed in-depth. All the hardware and software used, the approach in achieving the project, and the timeline of the project planning and managing are clearly described. Next, Chapter 4 focuses on the results obtained in the project with their respective explanations and theories behind. Lastly, the fifth chapter summarises the overall study, clarifies the limitations faced and proposes recommendations on future work for this project.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Literature reviews were done in the following sections to appraise the main reason for developing a personal safety and protection system, and the ideas, concepts, and techniques that are used in designing the system.

2.2 Personal Safety and Security

Personal safety is the most concerning issue when talking about travelling, where children are abducted, women are threatened, and senior citizens are abused. As the world is moving towards an urban lifestyle, travelling becomes a daily activity for everyone, either to school and university or to the workplace. However, the criminal offense level increases under the urbanisation of an area. High quality of life has resulted in a great cost of living, forcing some people that live at the foot of the social ladder to encounter financial and mental pressures. It cannot be denied that most of the women travellers are at the highest risk of victimisation and their level of fear while travelling especially alone has persuaded them to shift from the public to private transport usage (Rohana, Zaly and Hairul, 2013).

Crimes against women act as the largest threat to the personal safety of every woman around the world, including Malaysia. According to the Human Rights Commission of Malaysia (SUHAKAM) (2010), the first case in Malaysia that recognized sexual harassment at the workplace as an offence is the case of Jennico Associates Sdn. Bhd. vs. Lilian Therera de Costa in 1998. The victim claimed that she was subjected to sexual harassment both physically and verbally from her managing director. She eventually decided to resign from the position because this incident had made her suffer from emotional trauma. Through this case, it is affirmed that gender equity is the major morbid phenomenon to be handled seriously to overcome any violence against women.

Although the relevant authorities in almost every country in the world had introduced various laws against such crimes, the plight of women is not

likely to change. Rape, molestation, torture, kidnapping, and wife-beating have grown up over the years. In India, women are often treated as sex objects due to gender discrimination, which had led to the highest percentage of child marriages to be recorded for over 40 % in the world. As cited by Bhawana and Neetu (2014), one crime is reported every two minutes in India, in which one case of molestation is recorded to happen every 12 minutes and one case of rape is claimed to take place just every 21 minutes. The imbalanced development of the country has further exacerbated this problem. Women, who are unfortunate to be the victims of violence, may live in fear and psychological shadow throughout their lives. They tend to blame themselves for what had happened, resulting in depression and the possibility of committing suicide. Thus, crimes against women are well recognized as public health problems and human rights violations.

The personal safety of tourists becomes the primary factor while considering the development of the tourism industry. Bangkok, which is the capital of our neighbouring country – Thailand, is one of the international core tourism destinations. About 15.7 million international visitor arrivals were recorded in 2008 with a projection of 6 % from 2007 (Batra, 2008). Although the crime rate in Bangkok is considered relatively low as compared to many other tourist spots around the world, such as China and America, pickpocketing and robbery are getting more common in recent years. The income obtained from the tourism industry may be affected if these problems are not solved properly as tourists may suffer from the fear of victimisation and decide to stop visiting such a place full of criminals. A greater level of vigilance should be provided to ensure a hassle- and stress-free experience for every visitor to promise the return rate of foreign tourists that act as the major income for the country.

The Overseas Security Advisory Council (OSAC) of the USA (2020) encourages travellers in Malaysia, especially Americans to keep high alert on the crime and safety situation in Malaysia through an annual crime and safety report. It was highlighted in the report that the most common crimes in densely populated urban centres, such as Kuala Lumpur and Johor Bahru, include petty theft (especially pickpocketing), smash-and-grab theft from vehicles, and residential burglaries. Smash-and-grab theft often happens in a traffic jam,

where a pair of motorists will smash the window of the car, grab the valuables and speed off. Typically, the thieves focus on lone drivers as they do not have any resistance towards them. The victim can only let the offenders go out of sight helplessly. Moreover, a high volume of crimes is reported to happen at alleys and side streets near the main commercial zones after midnight. It is found that most of the incidents were targeted at lone victims, raising the personal safety issue in the world.

In short, personal safety and security is an arising issue all over the world that should be paid attention to preserve human rights not only for women, but for every person in the community. Everyone can enjoy a harmonious and peaceful lifestyle if not surrounded by potential crimes. To raise the personal safety and security level, some protection systems can play a significant role.

2.3 Protection System

In improving the personal safety of every high-risk group, researches on personal protection systems have been stimulated to grow rapidly these recent years. The emergence of pepper spray that required human effort to press on the opener to expel the gaseous pepper and shock generator that required the user's action to trigger the button can indeed help to decrease the unwarranted sense of fear and increase the safety and security level when an individual is walking alone on the street. However, crimes often take place in a sudden, in which victims will not have much time to respond by pressing on the pepper spray or triggering the button of the shock generator manually. This situation becomes worse when the surrounding condition is lack of light exposure. The victims may still be treated cruelly in the case that they fail to perform an effective response towards the criminals. Therefore, technology is implemented in producing a personal protection system that can carry out several actions automatically to protect the user.

In a project done by Ahir, et al. (2018), a wearable smart device was designed with the implementation of the IoT technology. This device can be started by tapping on the screen twice. The SOS message and GPS location will then be sent to the predefined emergency contacts automatically, and a buzzer that acts as an alarm will be triggered simultaneously. Along with the

smart device, there are two metal points installed on top of the screen to generate electric shock by emitting electric current. This feature can be helpful if the criminal is getting too close in contact with the victim, where unimaginable actions are going to occur. Nonetheless, this smart device possesses the drawback of lacking the false alarm prevention system due to the triggering method is being too simple. An unintentional activation will be triggered if the user does not put the smart device in a secured location. For example, if the user places the smart device inside a bag, mistaken activation may be carried out without notice from the user. A false alarm may be generated easily and a misunderstanding may occur.

Bankar, et al. (2018) had proposed a foot device as an effort of enhancing women's security. This device works in a way that it will be clipped onto the footwear of the user and triggered secretly by tapping the feet on the device at least ten times continuously within five seconds. Similarly, the latitude and longitude of the location will be traced by using the GPS module. The emergency message will be kept sending to the saved contact at an interval of 30 seconds to ensure that the emergency contact person notices the alert and the latest update of the user's condition. An extra feature is added in this device, where it can perform audio recording to act as proof later if required. At the same time, the buzzer will be triggered to alert the surrounding passers-by so that the user can obtain immediate help. There is also a small knife installed and attached to a DC motor for self-defence purposes, which will reveal itself when the system is activated. Yet, the activating method of tapping the feet for at least ten times in five seconds is a big challenge for the user in a nervous mood.

An intelligent device in the form of a wristwatch with a secret webcam that operates on the concept of "GEOFENCE" was proposed to provide extra safety for its user (Vahini and Vijaykumar, 2017). "GEOFENCE" is a virtual boundary pre-set in the protection system by the user, and this feature will trigger the system once the user moves out of the specified region marked previously. This device was programmed in such a way that a long beep sound at high volume will be generated at the receiver's side even if the device is in silent mode, with the prerequisite factor that the receiver must have the same device. This feature can ensure the alert messages from the victim are noticed

by the emergency contact to carry out subsequent actions as soon as possible. This wristwatch also consists of the feature of two-way talk, where it has the capability to receive any incoming call from the receiver. This can act as an alternative telecommunication tool when the phone is being stolen. But, this device must be first activated before the victimisation happens so that it can perform properly. Due to this reason, it is not a satisfactory solution to the personal safety problem as it is impractical to activate the device during an incident.

Vijaylashmi, et al. (2015) presented a design of a self-defence women safety system that is triggered by clicking on the physical switch on a wearable device. Similarly, this device possesses the functions of tracing the location of the user and sending it to the predefined emergency contacts. The special feature of this device is that it will play a prerecorded message using a speech circuit to raise the alert of surrounding people. This is much useful when the user's mouth is sealed and unable to speak out precisely and loudly. However, this feature may irritate the criminal to take violent actions in some cases. Besides, the activation of this device requires only a single press on the physical switch, which may result in an unexpected alarm due to accidentally pressing.

SMARISA designed by Sogi, et al. (2018) is activated by pressing on the physical button. Upon clicking, the current location of the victim is fetched, and the camera will capture the images of the attacker, which are then sent to the police or predefined emergency contact numbers via the victim's smartphone. This feature is very useful to store the proof of the incident, but it is highly dependent on the surrounding condition. A place where the illumination is insufficient will cause the images captured to blur. Besides, the camera is required to be held steadily to take clear pictures. This is quite impossible and impractical as the criminal will not stand still in a position as well as the victim will keep running away from the criminal, resulting in the vibration of the camera that will greatly affect the quality of the images taken.

Monisha, et al. (2016) also took an effort in the research of the protection system in improving the personal safety of every member of the community. They created a device called "FEMME" that is associated with an Android application. It can record audio and video of the incident to be used as

pieces of evidence. This device is installed with a radio frequency receiver to act as a hidden camera detector, which can detect any electromagnetic waves emitted from the spy camera. It is a creative feature to overcome the growth of sneak shot incidents, particularly towards single women. For example, an individual can stay in a strange place, like a hotel, without worrying about the presence of hidden cameras inside the room. Although this must be a great improvement in the personal protection system, the probability of getting error signals from the system is very high. This is because there are so many technological devices that will emit electromagnetic waves, which will influence the accuracy of the signal received.

A summary of protection systems developed by other researchers is listed in Table 2.1. A clear review of the characteristics and features of every system can be obtained from the table and a comparison can be made between them. These prototypes are used as the basis of the personal safety and protection system that is developed in this project.

Table 2.1: The summary of protection systems developed by other researchers.

No.	Devices by	Triggering Method	Devices	GPS	Sensors	Alarm	Shockwave Generator	Camera	Android Application
1	Ahir, et al. (2018)	Tap on the screen twice/ When being thrown with force detected.	Smart band	✔	Pulse rate, temperature, force	✔	✔	×	✔
2	Bankar, et al. (2018)	Tapping feet for a minimum of ten times within five seconds or with a one-touch switch system.	Foot device	✔	Pulse rate	✔	×	✔	✔
3	Vahini and Vijaykumar (2017)	Press on the smart band.	Smart band	✔	×	✔	×	✔	×
4	Vijaylashmi, et al. (2015)	Click on the physical button.	Smart band	✔	×	×	✔	×	×
5	Sogi, et al. (2018)	Click on the physical button.	Smart ring	✔	×	✔	×	✔	✔
6	Monisha, et al. (2016)	Press on volume button of the phone.	All-in-one device	✔	Radio frequency receiver	×	×	✔	✔

2.4 Speech Recognition

Speech recognition or automatic speech recognition (ASR) is a process of identifying words and phrases from spoken language and converting them into a machine-readable format (Desai, Dhameliya and Desai, 2013). In other words, it is the speech-to-text conversion. This technology is widely used for machines to respond accurately to human voices and provide various services, such as the “search by voice” function by Google, “Siri” by Apple, voice command function applied by in-car systems, and hands-free computing for disabled people. Speech recognition is growing fast due to the development of IoT. Almost all smart devices that emerge in the market today comprise the speech recognition function to connect themselves together, where a single command spoken to either one of the smart devices will trigger other smart devices to act upon the analysed words from the speech. A sample application that uses this technology is Google Home. The implementation of speech recognition technology in the IoT based personal safety and protection system will increase the reliability of the system.

A general speech recognition cycle starts with the transformation of the input of the speech signal. Then, frame blocking is carried out. The speech signal is divided into equally spaced blocks to obtain the signal characteristics. When examining over a short period, the signal characteristics are fairly stationary. However, over a long period, the characteristics of the speech signal change to reflect the different speech sounds. A string of phonemes can be produced by combining each block with the phoneme using the characteristics feature vectors. Next, spectrum analysis is applied to each block by using the bank of frequency filters, fast Fourier transform (FFT), and linear predictive coding technique. The phonemes produced have distinguished features that narrow the field for decision-making. Lastly, different algorithms will be applied to get higher accuracy results. An algorithm is constructed for each word of vocabulary and they are being compared with the string of phonemes to generate the result. The spoken speech is recognised into texts.

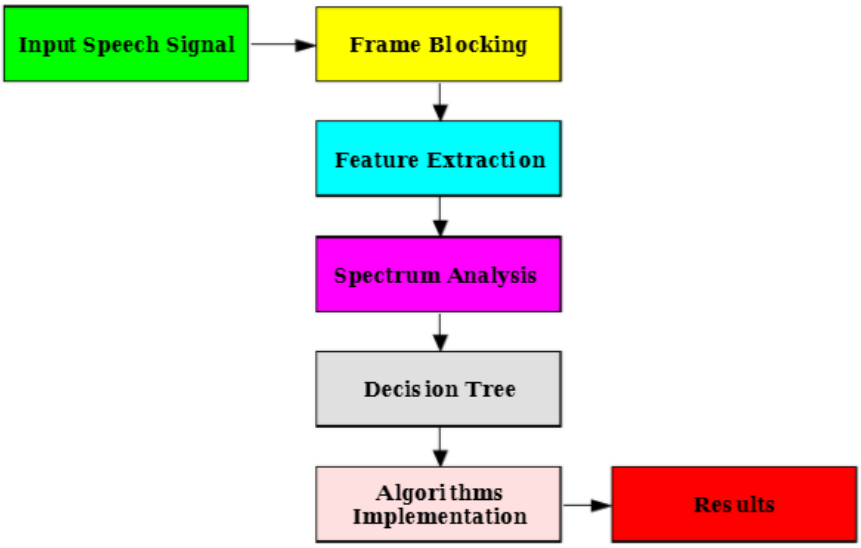


Figure 2.1: General speech recognition process (Shaikh and Deshmukh, 2016).

There are plenty of techniques used in speech recognition, including the acoustic-phonetic approach, artificial neural network-based approach, statistical-based approach, and many more. The acoustic-phonetic approach takes the assumption that there exist finite, distinctive phonemes in a speech-language. These phonemes are characterised by a set of acoustic properties that occur in a speech signal. For example, the English language consists of 40 different phonemes, which are independent of the vocabulary. This is the oldest technique of speech recognition that provides labels to the speech (Karpagavalli and Chandra, 2016).

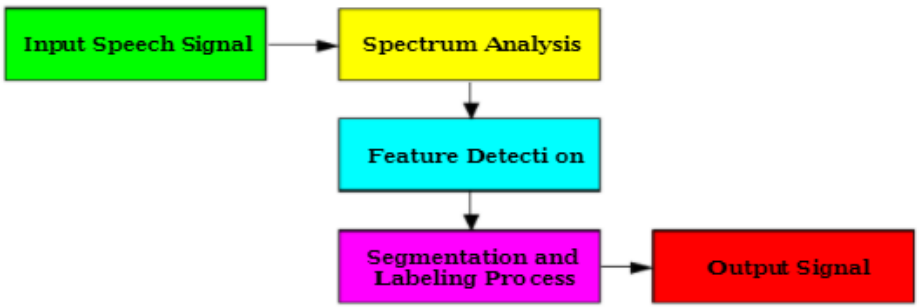


Figure 2.2: Block diagram of the acoustic-phonetic approach (Shaikh and Deshmukh, 2016).

The artificial neural network approach is suitable for complicated tasks, but inefficient when dealing with large vocabularies. The neurons that exist in the network are responsible to calculate the non-linear weight of inputs and broadcast the results to outgoing units. The pattern of values is assigned to input and output neurons, and the weight of strength of each pattern is determined by training sets.

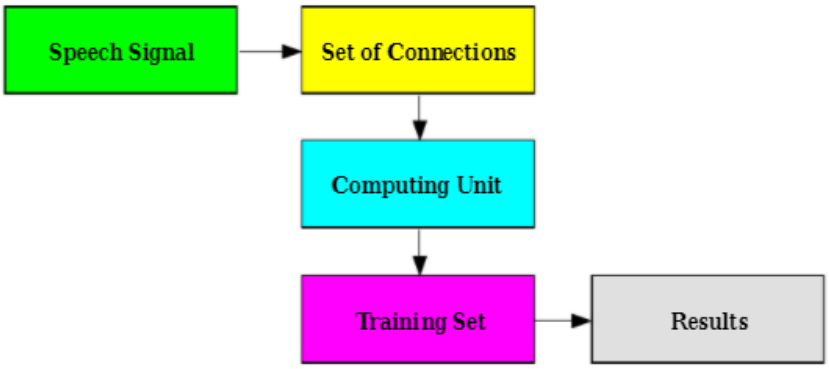


Figure 2.3: Block diagram of the artificial neural network approach (Shaikh and Deshmukh, 2016).

Hidden Markov Model (HMM) based approach is one of the statistical-based approaches that is the most efficient technique for speech recognition. It uses the best probabilistic model to perform non-deterministic selections depending on the characteristics of the input. This can remove the uncertainty that occurs in speech recognition, like confusable words, speaker variability, and mixing of sound. Before the HMM model is applied, the spoken speech must be extracted to features or coefficients. In HMM, the Gaussian distribution, state transition probabilities, mean, variance, and mixed weight for speech are taken into account for recognition, causing each phoneme to have different output distribution. By combining the individual train HMM for separate words or phonemes, a sequence of words or phonemes can be formed.

According to Iancu (2019), Google is the only cloud provider that offers ASR support for around 120 languages and dialects. In contrast, Amazon provides a cloud speech-to-text service called Amazon Transcribe that only supports five languages and dialects, including English, Portuguese, Spanish, Italian, and French. While for Microsoft, it only offers the speech-to-

text service in its Azure Cloud Service that can support six languages, which are English, Chinese, Spanish, Italian, German, and French. Thus, the Google Speech-to-Text Application Programming Interface (API) is the most suitable speech recognition tool among the others in terms of API. From the research done by Iancu (2019), as Google has a very large quantity of data stored on its servers and it owns a huge amount of machine learning algorithms, the Google Speech-to-Text API can perform better than other service providers.

A summary of some commonly used speech recognition techniques is shown in Table 2.2. The advantages and disadvantages of every technique are listed to establish a clear comparison between them. It can be concluded that the statistical-based approach with Hidden Markov Model (HMM) is the most effective and efficient method as it contains a relatively high volume of vocabularies that can train a large amount of data. The trained algorithms are also easily available. However, the Google Speech-to-Text API will suit this project of developing a personal safety and protection system better since the database and techniques it used are backed by Google, making it more accurate, reliable, and easy to use.

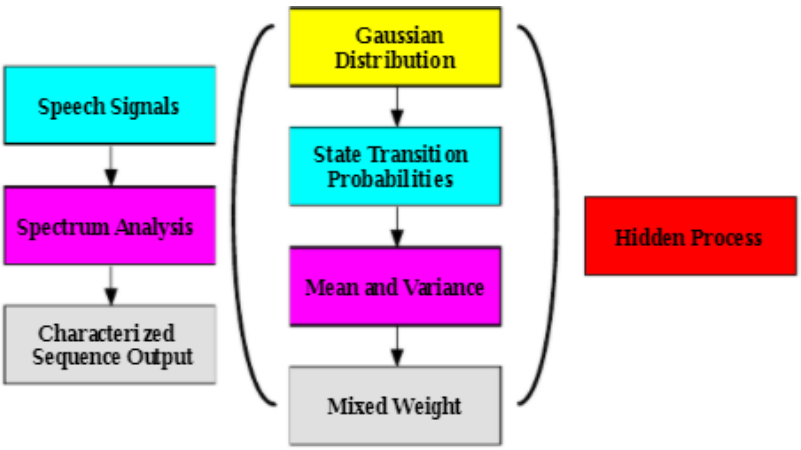


Figure 2.4: Block diagram of the Hidden Markov Model (HMM) based approach (Shaikh and Deshmukh, 2016).

Table 2.2: Comparative study of speech recognition techniques (Shaikh and Deshmukh, 2016).

Sr. No.	SRS Techniques	Advantages	Disadvantages
1.	Acoustic Phonetic Recognition	1. It reduces processing time for connected words.	1. Not widely used in commercial applications due to the large time execution of each isolated word.
2.	Dynamic Time Wrapping	1. Continuity is less important because it can match sequences with missing information. 2. Reliable time alignment between reference and test pattern.	1. It matches between two given sequences with certain restrictions. 2. It requires maximum time for complex computational work. 3. Limited number of templates.
3.	Pattern Recognition Approach	1. It recognizes patterns quickly, easily, and automatically because word-to-word matching will occur.	1. It is useful for word-to-word matching. 2. Template is the main problem. 3. Slow process. 4. It does not recognize speech if a new variation of pattern occurs.
4.	Vector Quantization Approach	1. It is useful for efficient data reduction.	1. It is text-dependent because it needs a codebook for matching.
5.	Template Base Approach	1. It is better for discrete words. 2. Fewer errors occur due to the segmentation and classification of small	1. Expensive due to the large vocabulary size in each word has reference templates for it. 2. Template matching and

		variable units.	preparation require more time. 3. It is difficult to recognize similar templates.
6.	Artificial Neural Network Approach	1. It can solve complex computational tasks effectively within less time. 2. It has the ability to automatically train the data and taught the system to change from the initial training model without error. 3. It can handle noisy, low-quality data efficiently and require minimum training data vocabulary.	1. It gives inefficient results for large vocabulary. 2. It is expensive because training it requires many iterations over a large amount of training data. 3. Full nature of the neural network is still not fully understood. 4. It requires more training time. 5. More error variation occurs due to the complex architecture of neural networks.
7.	Statistical Based Approach (Hidden Markov method)	1. The vocabulary size of HMM is very high so it can train a large amount of data. 2. It has an accurate mathematical framework. 3. The trained algorithms are easily available. 4. It can implement easily and anyone can easily change the size, type, and architecture of these models to suit a particular	1. A significant increase in computational complexity. 2. Need a large amount of data.

		word. 5. It is more robust because the probability of certain words can occur next to each other. 6. It has the capability to achieve recognition rates accurately. 7. It has an efficient learning algorithm. 8. It has a flexible and general model for sequence properties. 9. It can learn variable data unsupervised.	

2.5 Overview of the Internet of Things (IoT)

In the past decade, the Internet has become ubiquitous, touching almost every corner of the world. Human life has transformed in an incredible way, in which everything can now interact with each other to perform a specific purpose with the Internet. The Internet of Things, abbreviated as IoT, is defined as a communication between the physical and digital worlds (Vermesan, et al., 2011). The physical world consists of a wide variety of sensors, which detect mechanical changes and convert them into electrical signals, as well as actuators, which receive electrical energy to produce mechanical outputs. With IoT technology, the digital world can interact with the physical world for the purpose of monitoring, controlling, and analysing. Another definition by Peña-López, et al. (2005) states that the Internet of Things acts as a paradigm, where networking and computing capabilities are embedded in any feasible object. These capabilities can be used to monitor the state of an object or to manipulate its state remotely. In short, the IoT refers to a new technology that every electronic device is connected through a similar network. All devices connected to the network can be commanded to perform a particular task together. A variety of sectors make use of IoT technology to

enhance the infrastructure, especially in telecommunication and location tracking.

2.5.1 Three-layer Architecture

Three-layer architecture is the most basic architecture for IoT. It is the first architecture introduced in the early stage of research in this area. As mentioned in its name, there are three layers, that are perception, network, and application layers in this architecture (Mashal, et al., 2015). The perception layer is the physical layer consisting of sensors to carry out the purpose of sensing and gathering information about the surrounding environment. Various physical parameters can be measured and identified, such as movement, temperature, pressure, and humidity. Since sensors are transducers that transform power from mechanical into electrical, the information obtained will be converted into an electrical or digital signal to prompt the subsequent action. The network layer functions as a linkage to connect all the devices to other network devices and servers for carrying out data transmitting and processing. Normally, the information obtained from sensors will be transferred into cloud storage to prepare for later application. Lastly, the application layer is responsible for delivering specific services or actions based on the analysis done on the information collected. This is the last step to define various applications to achieve the mission of a system. The actuator is one of the major components in this layer. For example, a smart home system is an application generated after analysing the relevant information acquired by sensors through a wireless network protocol. There is no physical linkage or connection between the devices in the smart home system. Thus, all communication among devices and appliances is performed through a wireless network.

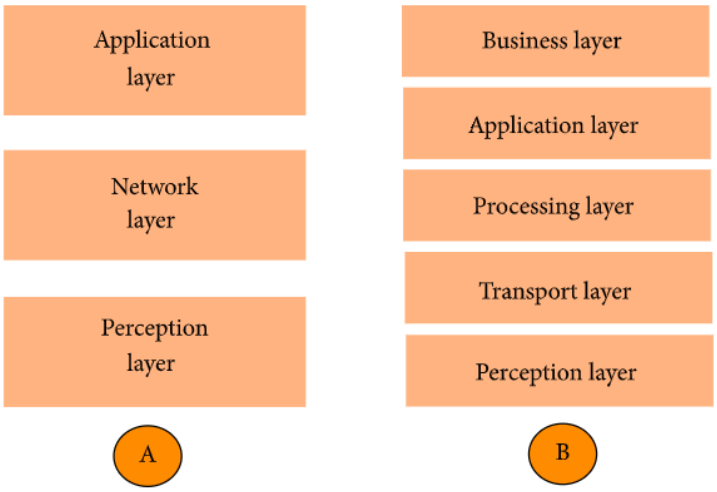


Figure 2.5: Three-layer and five-layer architectures of IoT (Sethi and Sarangi, 2017).

2.5.2 Five-layer Architecture

Although the three-layer architecture can represent the main idea of IoT technology, finer aspects are required to be focused on to further develop a perfect IoT system. Due to this reason, the five-layer architecture is introduced based on the basic three-layer architecture with the addition of processing and business layers. From Figure 2.5, the five-layer architecture of IoT contains perception, transport, processing, application, and business layers, where the roles of both the perception and application layers remain unchanged (Khan, et al., 2012). The transport layer performs a similar job with the network layer in the three-layer architecture, but it is now transferring the information and data obtained from the perception layer to the processing layer (normally a cloud or server storage), or vice versa through various networks, such as Wireless Fidelity (Wi-Fi), Bluetooth, local area network (LAN), and Third Generation (3G). Next, the processing layer, which is also recognized as the middleware layer, stores, analyses, and processes the sensor data from the transport layer. This layer can typically manage and offer a variety of services to the lower layers. Many technologies, including cloud computing, databases, and big data processing modules are employed in this layer. Last but not least, the business layer takes the responsibility to control the entire IoT system and its activities. Normally, the applications, business and profit models, and users' privacy are managed and secured in this layer. Thus, it is a significant layer to ensure the

safety and security of the IoT system, preventing any disclosure or leaking of users' information.

2.5.3 Cloud-based Architecture

There are two types of IoT system architectures, including cloud and fog computing. This classification is done based on protocols that make it different from the classification of three- and five-layer architectures. Data processing can be done by applying both system architectures. In cloud computing, data processing is usually performed in a large centralized fashion by using cloud computers. Such a cloud-centric architecture places the cloud at the centre, with applications at the top and the network of smart things at the bottom (Gubbi, et al., 2013). Cloud computing is widely used in IoT technology as it provides great flexibility and scalability, where developers can perform data storing, data mining, data analysing, data visualisation, and machine learning through the cloud.

2.5.4 Fog-based Architecture

On the other hand, fog computing differs from cloud computing in the sequence of data processing. In fog computing, sensors and network gateways will carry out some of the data processing and analytics in prior. Four additional layers are inserted between the physical and transport layers, namely monitoring, preprocessing, storage, and security layers. The monitoring layer will conduct the supervising jobs on either the responses or errors of all devices within the IoT system. The filtering, processing, and analytics of data will then be executed in the preprocessing layer. The processed data is temporarily stored in the storage layer before sending it into the cloud, whereas the security layer performs encryption or decryption of data to make sure that the data integrity and privacy are secured. The major difference between cloud computing and fog computing is that the information and data obtained are directly uploaded into cloud storage to be processed later in cloud computing, but it is processed in advance in fog computing to exert a stronger guarantee on the data accuracy and security. Generally, the IoT system used for business purposes prefers fog computing because the data is

collected on a large scale that might require prior filtering and processing so that only useful data is stored for analytics.

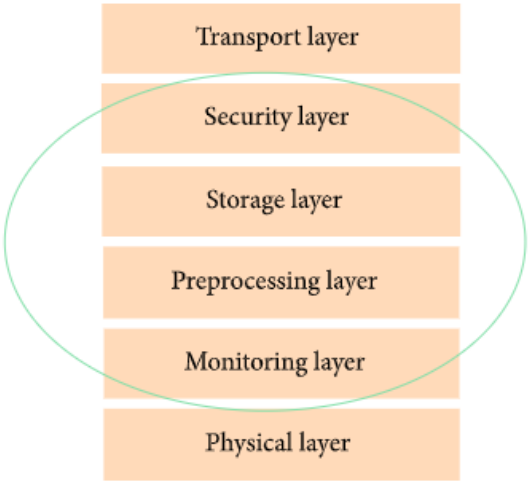


Figure 2.6: Fog architecture of a smart IoT gateway (Sethi and Sarangi, 2017).

2.6 Wireless Network Protocols

A wireless network is the new technology of networking in which data signals are transferred through the air. No physical connection with cables or wires is required to perform wireless networking. The wireless network works in the principle of sending and receiving the electromagnetic waves propagated through the radio frequencies generated by antennas. There are four main categories of wireless networks:

(i) Wireless Wide Area Networks (WWANs).

(ii) Wireless Metropolitan Area Networks (WMANs).

(iii) Wireless Local Area Networks (WLANs).

(iv) Wireless Personal Area Networks (WPANs).

Table 2.3: Comparison of wireless network types (Sharma and Dhir, 2014).

Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas

Table 2.4: Comparison of characteristics of different wireless protocols (Saad, et al., 2014).

Protocols	**Bluetooth**	**UWB**	**ZigBee/IP**	**Wi-Fi**	**Wi-Max**	**GSM/GPRS**
Frequency band	2.4 GHz	3.1 – 10.6 GHz	868/915 MHz; 2.4GHz	2.4; 5 GHz	2.4; 5.1 – 66 GHz	850/900; 1800/1900 MHz
Max signal rate	720 Kb/s	110 Mb/s	250 Kb/s	54 Mb/s	35 – 70 Mb/s	168 Kb/s
Nominal range	10 m	10 – 102 m	10 – 1000 m	10 – 100 m	0.3 – 49 km	2 – 35 km
Nominal TX power	0 –10 dBm	-41.3 dBm/MHz	-25 – 0 dBm	15 – 20 dBm	23 dBm	0 – 39 dBm
Number of RF channels	79	(1 – 15)	1/10; 16	14 (2.4 GHz) 64 (5 GHz)	4; 8 10; 20	124
Channel bandwidth	1 MHz	0.5 – 7.5 GHz	0.3/0.6 MHz; 2 MHz	25 – 20 MHz	20; 10 MHz	200 kHz
Modulation type	GFSK, CPFSK, 8-DPSK, π/4- DQPSK	BPSK, PPM, PAM, OOK, PWM	BPSK, PPM, PAM, OOK, PWM	BPSK, QPSK, OFDM, M-QAM	QAM16/64, QPSK, BPSK, OFDM	GMSK, 8PSK
Spreading	FHSS	DS-UWB, MB-OFDM	DSSS	MC-DSSS, CCK, OFDM	OFDM, OFDMA	TDMA, DSSS
Basic cell	Piconet	Piconet	Star	BSS	Single-cell	Single-cell
Extension of the basic cell	Scatternet	Peer-to-Peer	Cluster tree, Mesh	ESS	PTMP, PTCM, Mesh	Cellular system
Max number of cell	8	236	> 65000	2007	1600	1000

nodes						
Encryption	E_0 stream cipher	AES block cipher (CTR, counter mode)	AES block cipher (CTR, counter mode)	RC4 stream cipher (WEP), AES block cipher	AES-CCM cipher	GEA, MS-SGSN, MS-host
Authentication	Shared secret	CBC-MAC (CCM)	CBC-MAC (ext. of CCM)	WPA2 (802.11i)	EAP-SIM, EAP-AKA, EAP-TLS or X.509	PIN; ISP; Mobility Management (GSM A3); RADIUS
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC	AES based CMAC, MD5-based HMAC, 32-bit CRC	GPRS-A5 Algorithm
Success metrics	Cost, convenience	Throughput, power, cost	Reliability, power, cost	Speed, Flexibility	Throughput, Speed, Range	Range, Cost, Convenience
Application focus	Cable replacement	Monitoring, Data network	Monitoring, control	Data network, Internet, Monitoring	Internet, Monitoring, Network Service	Internet, Monitoring, control

2.6.1 Wireless Local Area Networks (WLANs)

This type of wireless network allows the user in a local area, such as a building, to form a common network that grants access to the Internet. IEEE 802.11 is a standard body that helps in coordinating and promoting data networking standards. It enables vendors to create compatible products by defining the mechanical process of implementing WLANs in the 802.11 standards. It specifies key management and security association management plus access control, data confidentiality, and data integrity. Wi-Fi is a kind of wireless network classified under the WLANs. It is usually used to convey information over a long distance of about 100 metres with the maximum signal rate of 54 Mbps for anyone having the access codes or passwords into the Wi-Fi network. However, it possesses the drawback of being easily affected by interference, like electromagnetic waves emitted from any electronic device.

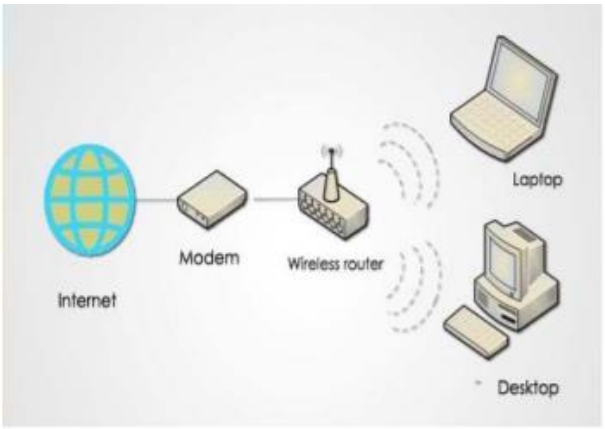


Figure 2.7: Wireless Local Area Network (Sharma and Dhir, 2014).

2.6.2 Wireless Personal Area Networks (WPANs)

This type of wireless network allows users to communicate between a wide range of devices that is small and power-efficient. Bluetooth, ZigBee, and Ultra-Wideband (UWB) are examples of WPANs. They can usually be used to convey information over a short distance of about 10 metres among a private group of participant devices. Unlike the WLANs, connections over the WPANs involve no infrastructure, where a direct connection can be carried out among the devices having WPAN technology. The maximum signal rate is only 720 Kbps in Bluetooth, 250 Kbps in ZigBee, and 110 Mbps in UWB. ZigBee technology is normally applied in home automation that needs only a

low data transfer rate to fulfil the simple requirement. On the other hand, UWB technology is getting more attention as it can replace the high-speed serial bus, such as USB 2.0 to deliver data much faster in home networking.

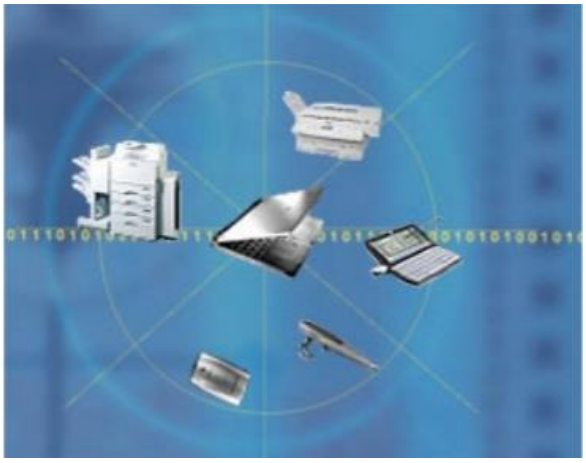


Figure 2.8: Wireless Personal Area Network (Sharma and Dhir, 2014).

2.6.3 Wireless Metropolitan Area Networks (WMANs)

This type of wireless network allows users to interconnect multiple networks within a metropolitan area, such as different buildings within a city, that acts as an alternative for fibre cabling. It can convey information over a very long distance of up to 50 kilometres with a maximum signal rate of 70 Mbps. Worldwide Interoperability for Microwave Access (WiMAX) is the most popular wireless technology in this category. The common application is the mobile broadband that provides high bandwidth over long-range transmission.

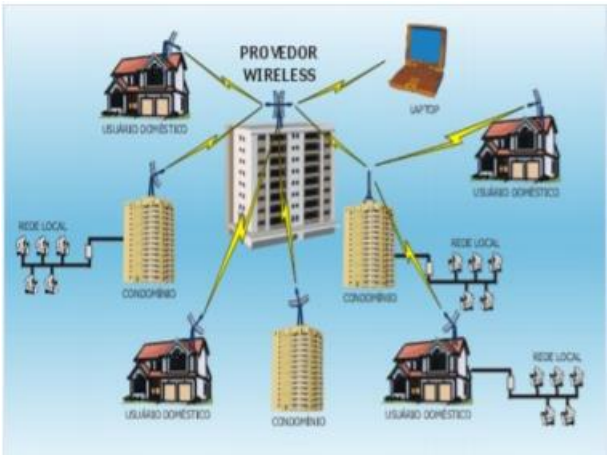


Figure 2.9: Wireless Metropolitan Area Network (Sharma and Dhir, 2014).

2.6.4 Wireless Wide Area Networks (WWANs)

This type of wireless network can provide a connection over large areas, such as between cities or even countries. General Packet Radio Service (GPRS), GSM, and Universal Mobile Telecommunication System (UMTS) are examples of applications through WWANs, which can convey information at the maximum signal rate of 168 Kbps.

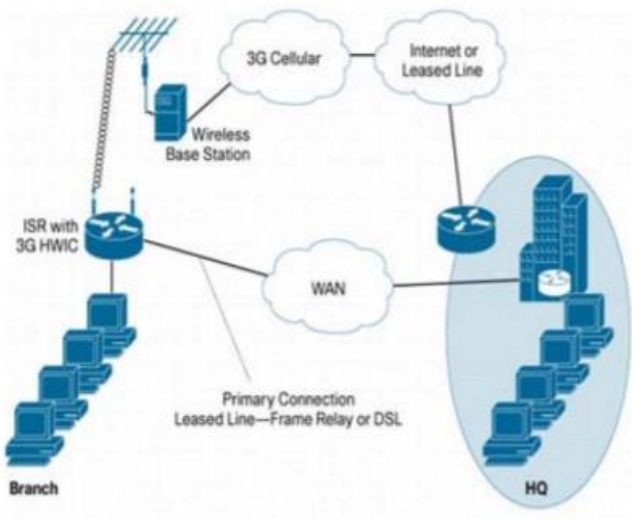


Figure 2.10: Wireless Wide Area Network (Sharma and Dhir, 2014).

CHAPTER 3

METHODOLOGY AND WORK PLAN

3.1 Introduction

In this section, the methodology of the project will be discussed with all necessary details provided to repeat this project and obtain reproducible results. The materials and facilities used in accomplishing the objectives will be elaborated and justified through the investigation done.

3.2 Planning and Managing of Project Activities

Tables 3.1 and 3.2 show the Gantt chart for parts I and II of this project. Part I of the project is mainly focusing on the problem formulation, literature review, and findings for conceptual design, whereas part II of the project emphasises on hardware and software design, prototype development, and report writing.

Four major activities were completed in part I of this project. In the first two weeks, a thorough discussion was held with the project supervisor, Mr. Chai to study the project requirements and define the broad outcomes that are expected to be achieved by the time the project ends. During the meeting, the specific outputs and activities to be carried out in part I of this project were planned to cope with the expected project outcomes smoothly. Some suggestions on the project design from the aspects of its features and functions were given by Mr. Chai to establish a rough idea and concept of the personal safety and protection system to be built. The Gantt chart shown in Table 3.1 was prepared in the second week as well to ensure all the activities to be performed were well-scheduled and organised.

After that, a comprehensive literature review was conducted to synthesize other researchers' ideas on the topic to generate useful ideas for adding attractive features to the project. Since this is not a new topic, some unique features must be implemented to act as selling points of the project developed. Therefore, plenty of available works had been compared and contrasted to discover the limitations that exist in their projects. Some possible features and functions were evaluated to find out their suitability to be included in this project to minimise the drawbacks of existing similar devices

and maximise the achievement of the objective of providing personal protection to an individual during an emergency condition. The methodology of this project was determined in the sixth week after a detailed analysis was done from reviewing the other researchers' works. Eight weeks were spent on doing the literature review.

Starting from the eighth week, conceptual design and component selection were executed. The types of hardware (electronic components and processing unit) and software (programming language, cloud server platform, and IDE) used in designing the project were proposed. Every component that performs a particular job towards achieving the specific feature was selected after filtering similar components available in the market. The most suitable items were adopted instead of the best items so that the proposed features and functions can be realised with optimal power consumption and performance. This is because a higher performance component will definitely utilise a greater power and thus generating more heat. This condition is not favourable since the device to be produced is considered quite simple, where medium-end components are sufficient to support the purpose. Preliminary testing was done on the application of components to ensure each of them can help in reaching the objectives. This milestone took around six weeks to finish.

Throughout part I of the project, many ideas and concepts were collected to be documented in this report. Five weeks were spent in the report writing. This report was revised several times before submission to make sure there is no grammatical error. Since the report for part I of the project is just a progress report of the entire project, only brief information is provided for the methodology and result sections. The oral presentation was carried out in the last week of part I of the project to convey the central idea of this project and the up-to-date progress of part I.

Table 3.1: Gantt chart for part I of this project.

No.	Project Activities	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14
M1	Problem formulation & project planning														
M2	Literature review														
M3	Conceptual design & component selection														
M4	Report writing & presentation														

However, some modifications had been done in part II of the project to solve the difficulties encountered. There are six major activities to be completed in part II of this project. At first, hardware testing and programme development were conducted together to coordinate a good interaction between the software and hardware. Programme for controlling all the hardware was written in Python inside the Raspberry Pi 3 Model B+, including the codes to obtain inputs from every sensor, store the data into the cloud server, and retrieve the data for specific actions and analysis. This is the longest stage of the project because several methods were tried and tested to produce the perfect prototype.

In the eighth week, data analysis and Android graphical user interface (GUI) development were started at the same time so that the prototype can be tested and debugged in experiments. Data analysis functions to ensure all the data collected from the system is accurate and precise, while the Android GUI will act as the user interface of the system to carry out various settings and preferences as well as monitor the condition of the system. Data to be presented in the Android application is directly retrieved from the cloud server to realise real-time monitoring and support. Multiple times of corrections were done to the software design until the prototype can perform up to the expectation.

The poster preparation began in the tenth week. The poster includes all the relevant and useful information, especially the result and discussion of the project to present and promote the prototype developed. Lastly, documentation of the project was carried out. The final report writing was started in the eighth week, which is two weeks earlier than in part I of this project. More time is assigned to produce a high-quality report that can be used by others to repeat this project and obtain identical, reproducible results. The final report must be comprehensive so that it can deliver knowledge to the readers effectively. The period devoted to the final report writing was continued until the fourteenth week. Lastly, the final presentation will be prepared and conducted to present the outcomes of this project.

Table 3.2: Gantt chart for part II of this project.

No.	Project Activities	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14
M1	Hardware testing														
M2	Programme development														
M3	Data analysis														
M4	Android GUI development														
M5	Poster preparation														
M6	Report writing & presentation														

3.3 System Architecture

The proposed system consists of four major parts, namely the sensing unit, processing unit, actuating unit, and visualising unit. From the block diagram in Figure 3.1, the sensing unit comprises all the sensors and receivers, including the capacitive touch sensor, USB microphone, and IMU sensor, that are responsible for collecting inputs of the system. While in the processing unit, the Raspberry Pi 3 Model B+ running on the Raspbian operating system (OS) is the only processor used to control the operation of the whole system. A USB to TTL converter module is applied to generate another set of Universal Asynchronous Receiver/Transmitter (UART) pins to communicate with the GPS tracking module. The processing unit plays the role of receiving data obtained from the sensors and receivers, and performs the proper actions after analysing the information collected. If the user is in danger, the actuating unit will be triggered to get the real-time location of the user and synchronise every detail gathered into Firebase Cloud Server. The data will then be immediately sent to the emergency contacts pre-set by the user to seek for help. At the same time, the buzzer will be triggered to alert the passers-by about the incident that is going to happen or already happened. Instant help can be provided to the user by the surrounding people and the victimisation can be avoided. Lastly, the visualising unit is the real-time user interface that will provide the real-time sensors' data and the nearest safe location, such as the police station through the Android application. A mis-triggered alarm can also be cancelled in the Android application. Data attained will be stored in the cloud server for future statistical study and can even act as shreds of evidence to the incident.

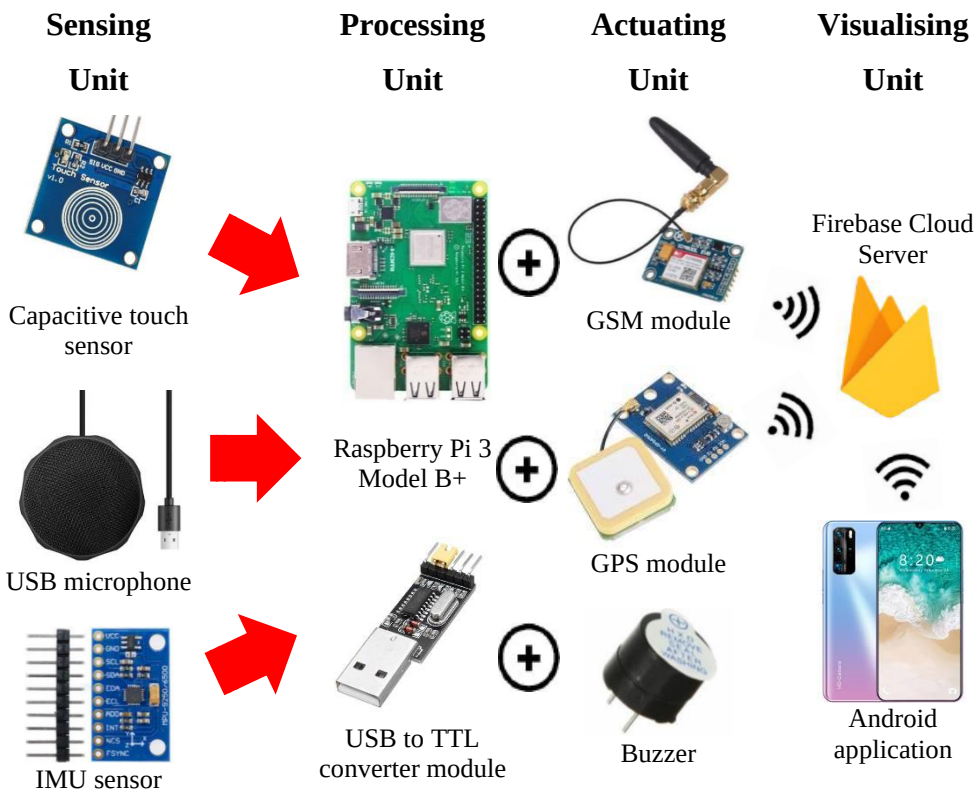


Figure 3.1: The block diagram of the personal safety and protection system.

3.4 Hardware

All the hardware used in developing the system is discussed in the following subsections.

3.4.1 Raspberry Pi 3 Model B+

The primary processing unit used in this system is the Raspberry Pi 3 Model B+ as shown in Figure 3.2. It is a single-board computer known for its credit-card-size with dimensions of 85 mm × 56 mm × 17 mm. It contains a 64-bit quad-core processor running at 1.4 GHz, which is 0.2 GHz faster than the previous generation. With extended 40-pin general-purpose input/output (GPIO) header, this micro-computer is more than enough to handle all the connections between components and perform the background programme smoothly. Since the protection system is designed to work non-stop for 24 hours per day, the Raspberry Pi 3 Model B+ is powerful enough to manage all the operations on-going simultaneously. The power consumption characteristic of this micro-computer meets the requirement of the system, where a 5V/2.5A power source is sufficient to power it. As it is a mobile protection system, high

power-efficient is preferred so that the system can be powered with a portable battery. In this project, a 20000 mAh power bank will be connected to act as the power supply of this micro-computer via a micro USB connector.

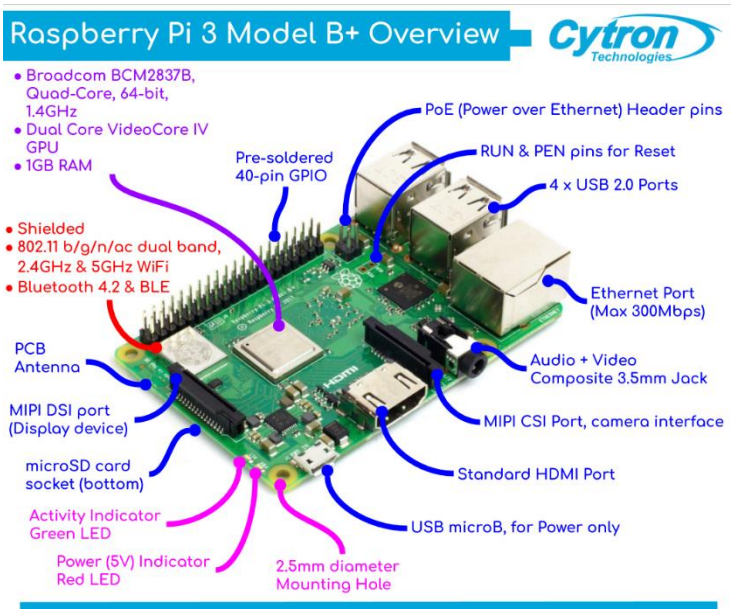


Figure 3.2: Overview of the Raspberry Pi 3 Model B+ (Cytron Technologies, n.d.).

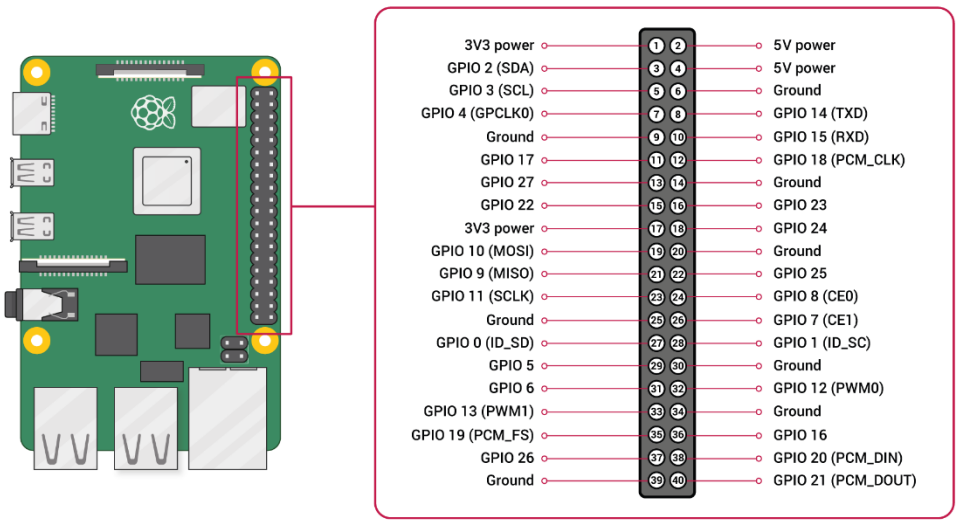


Figure 3.3: Raspberry Pi 3 Model B+ pinouts (Raspberry Pi Foundation, n.d.).

3.4.2 CH340G USB to TTL Converter Module

Since both GSM and GPS modules require UART pins to transmit and receive information, the only set of UART pins on the Raspberry Pi 3 Model B+ is not sufficient. Hence, a CH340G USB to TTL Converter Module is introduced into the system to receive the data from the GPS module. Although software serial of converting the normal pins on the Raspberry Pi 3 Model B+ into the UART pins can be done by programming, the signal is not stable and will affect the performance of the whole system if the connection is lost. A hardware USB to TTL converter module will not encounter this problem. It can be simply connected through the USB port of the Raspberry Pi, and retrieve data from the GPS module instantly under the maximum baud rate without performing any setting.

Figure 3.4: CH340G USB to TTL Converter Module.

3.4.3 TTP223 Capacitive Touch Sensor

A TTP223 Capacitive Touch Sensor is a touchpad detector integrated circuit (IC) that offers a one-touch key. It is used in this system to replace the traditional direct button key for triggering the system. With only 0.5 seconds of stable time after power-on, this touch sensor can respond rapidly with the maximum response time of 60 ms towards the input within the range of 0-50 pF capacitance. The failure of triggering the system due to the technical problem of a traditional mechanical button can be prevented by using this touch sensor. Also, the false alarm can be avoided when the triggering condition is set to apply an input to the touch sensor for more than five seconds, making it ideal for this system. This triggering method is user-

friendly and simple, but difficult in activating a false alarm. In the case of a false alarm, it can be cancelled by applying only one second of continuous input to the touch sensor. Thus, any mistrigerring of alarm can be stopped immediately.

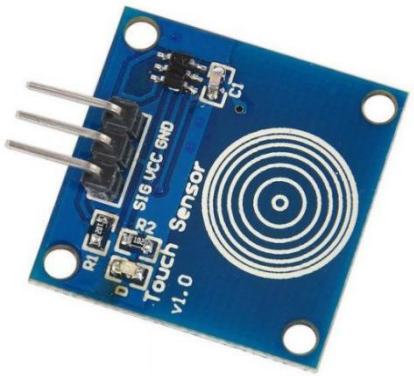


Figure 3.5: TTP223 Capacitive Touch Sensor.

3.4.4 USB Omnidirectional Microphone

An omnidirectional microphone is a microphone that picks up sound with equal gain from all sides or directions of the microphone. This is in contrast to unidirectional microphones, which pick up sound with high sensitivity only from a specific side. Figure 3.6 shows the typical polar plot response of an omnidirectional microphone. Since it has a circular polar plot due to it records sound from all directions (0º to 360º), it allows greater flexibility in the directionality of sound pick-up. During an emergency, the user can just speak to the microphone without regard to the position of the microphone. This USB omnidirectional microphone possesses a pick-up distance of 50-200 cm with a sensitivity of 52 dB, which is appropriate in the usage of this project because the normal human conversation is about 50 dB (Victory, 2019). Besides, it has a signal-to-noise ratio of 78 dB that is considered excellent as compared with other microphones. As it is USB-based, it can be connected directly to the USB port of the Raspberry Pi 3 Model B+, making a very simple connection.

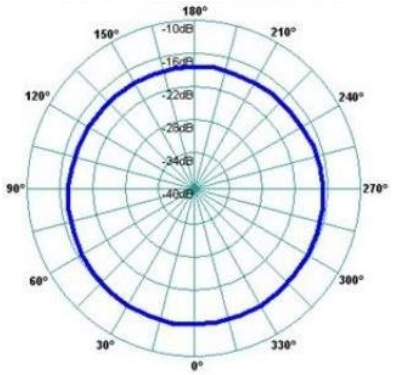


Figure 3.6: The polar plot of an omnidirectional microphone.

Figure 3.7: USB Omnidirectional Microphone.

3.4.5 MPU9250 9-axis IMU Sensor

The MPU9250 9-axis IMU Sensor has nine motion sensing axes with minimal cross-axis sensitivity between the gyroscope, accelerometer, and magnetometer axes. This sensor module combines the gyroscope, accelerometer, and magnetometer in a single board, in which it can measure the orientation, angular velocity, acceleration force, and magnetism. Besides, there is also an embedded temperature sensor on this sensor module with a measurement range of -40 ºC to 85 ºC. Through these measurements, the system can detect whether the user is in normal moving speed and orientation, and obtain the temperature of the surrounding environment. If there is a sudden change in any of these parameters that exceed the threshold and it is maintained for more than 30 seconds, it can be guessed that the user is in danger, the device is being thrown, or there is a fire disaster happening around the user. Analysis can be done to trigger the protection system.

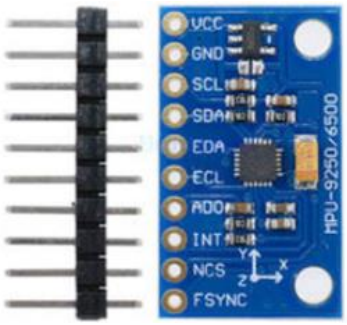


Figure 3.8: MPU9250 9-axis IMU Sensor.

3.4.6 Buzzer

A buzzer is installed in the system to alert the passers-by that the user is in danger. It can produce an alarm of up to 85 dB, which is loud enough to create a sense of fear to the criminal to stop their improper actions.

Figure 3.9: Buzzer.

3.4.7 GY-NEO6MV2 GPS Tracking Module

The GY-NEO6MV2 GPS Tracking Module is a stand-alone GPS receiver built-in with electrically erasable programmable read-only memory (EEPROM) for saving data when it is powered off. The baud rate of this module is 9600, indicating that it is capable of transmitting a maximum of 9600 bits of data per second. There is a rechargeable button battery on this module that acts as a backup battery when the power supply drains out. The location data can still be collected and analysed by the system although the power source is used up. Thus, this GPS module is much compatible with the applications of the protection system.

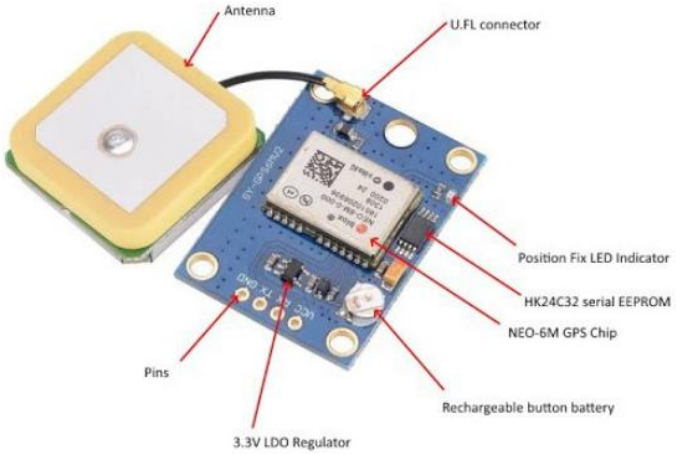


Figure 3.10: GY-NEO6MV2 GPS Tracking Module.

3.4.8 SIM800L GSM Module

The SIM800L GSM module supports quad-band communication, including 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz. Voice, short message service (SMS), and data information can be transferred through the GPRS with low power consumption. GPRS is a packet-based wireless communication service that transmits data at rates from 56 Kbps to 114 Kbps and promises continuous connection to the Internet. For this module, it is rated with GPRS class 12, which can transmit data at a maximum of 85.6 Kbps. This transmission rate is more than enough to send the data collected from the sensors over the cloud server to be analysed for generating proper actions of the protection system.

Figure 3.11: SIM800L GSM Module.

3.5 Software

All the software used in developing the system is discussed in the following subsections.

3.5.1 Firebase Cloud Server

In order to achieve a real-time response of the protection system, the data obtained from the sensors must be stored and analysed immediately from time to time. This is to always prepare the system in a stand-by mode for actions to be carried out to cope with the dangerous situation faced by the user. Firebase is a cloud server platform that allows the synchronisation of data in real-time and establishes communication between devices. This platform provides the features of the real-time database, performance monitoring, analytics, messaging, and crash reporting that fully suits the project objectives. Since Firebase is backed by Google, the security of this platform is said to be on the highest level. The personal data from the user can be protected well and free from the risk of being hacked. Moreover, Firebase can be simply linked with the Android Studio IDE that makes the development of the system's mobile application easier. There is an attractive feature offered by Firebase, where the Realtime Database Software Development Kits (SDKs) will store the data in the local cache of the system when the device is gone offline. The synchronisation of data will continue automatically once the device is backed online.

Figure 3.12: Firebase cloud platform powered by Google (Google Developers, n.d.).

3.5.2 Visual Studio Code

The Visual Studio Code is used as the major programming software in this project. It gives the function of accessing the Raspberry Pi 3 Model B+ remotely through Secure Shell (SSH) protocol. According to SSH.com (n.d.),

the SSH protocol is a method for secure remote login from one computer to another. Since the Raspberry Pi 3 Model B+ is considered a mini-computer, it comes with this communication protocol. Normally, the SSH protocol provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. Thus, using the Visual Studio Code to perform the SSH communication with the Raspberry Pi 3 Model B+ is considered very safe and secured, and the programme code can be easily debugged with the strong debugging engine in the Visual Studio Code.

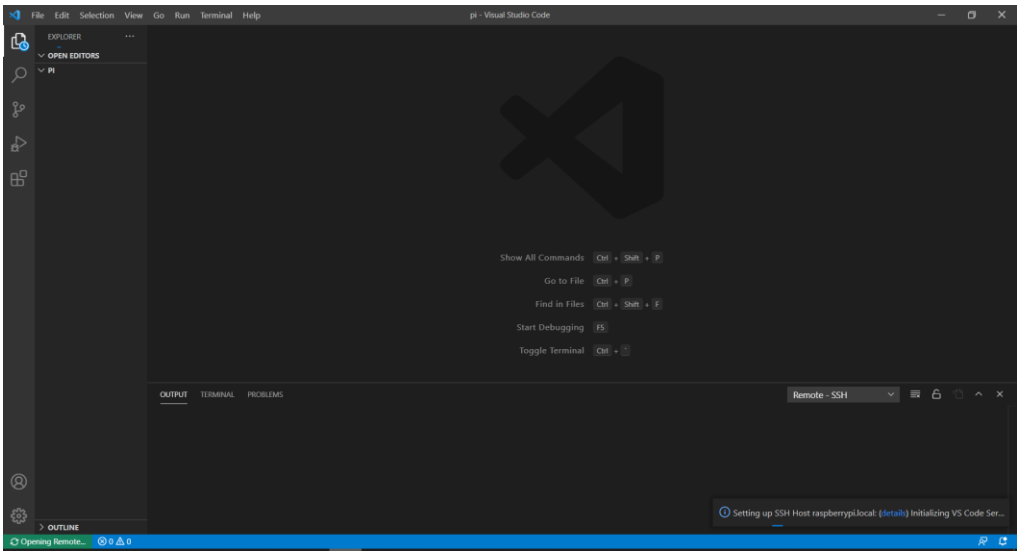


Figure 3.13: The Raspberry Pi 3 Model B+ is connecting to the Visual Studio Code through the SSH protocol.

3.5.3 Android Studio IDE

The Android Studio IDE is used to develop an android application to act as a graphical user interface (GUI) of the system. The programming language used to write the backend script is Java, while the GUI is designed by Extensible Markup Language (XML). In this IDE, virtual debugging and visualization of the developed application can be done through a simulated phone. With just a click, the android application built by this IDE can be directly linked to Firebase to perform real-time data storage and analysis. Since this IDE is an open platform, plenty of tutorials are available online for free, which makes the development process of the application easier.

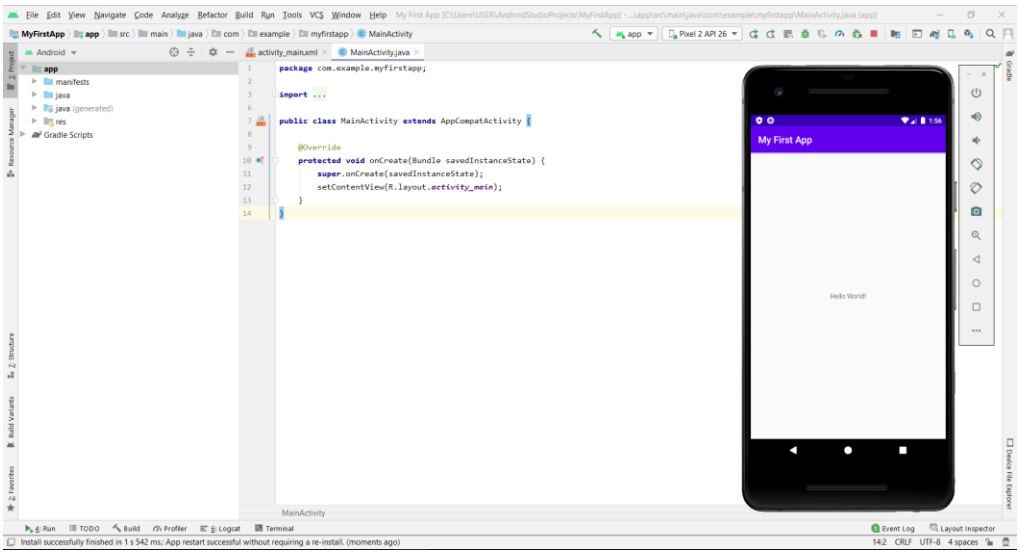


Figure 3.14: Android Studio IDE.

3.5.4 Fritzing

In doing the circuit design, the Fritzing software is chosen because it is an open-source platform, where the user can simply create any electronic component on his preference. Hence, a lot of components can be searched online, making the circuit designing job easier. Besides, it also offers multiple types of circuit diagram views, such as virtual part view, schematic view, and printed circuit board (PCB) view. This can enhance the understanding of the user by providing better visualization of the design so that the project can be repeated and similar reproducible results can be obtained.

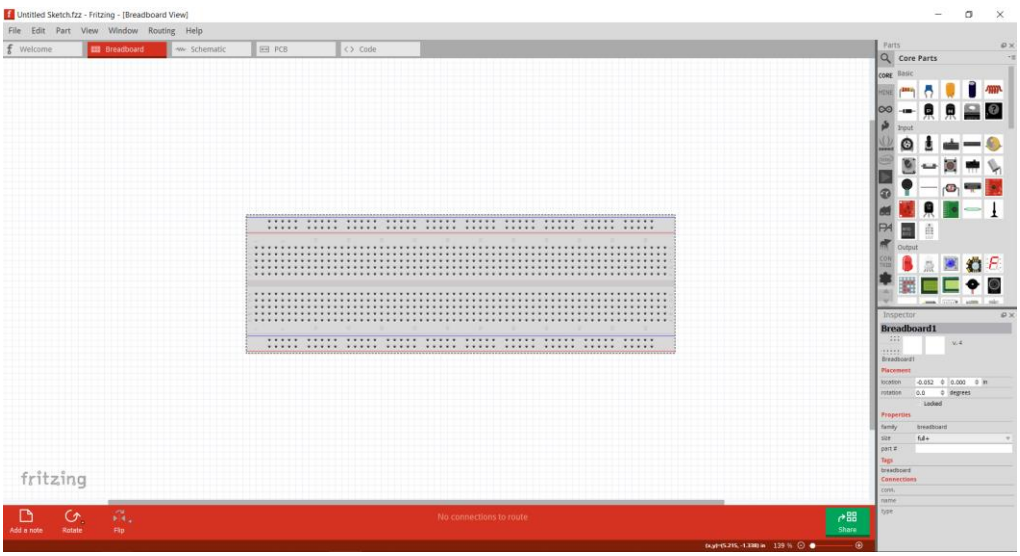


Figure 3.15: The fritzing software.

3.6 Overall System Flowchart

The logical flow of the developed system is as shown in Figure 3.16. Upon turning on the system, the GPIO pins 22 and 23 are set to be the signal pins for the touch sensor and buzzer respectively. Since the calculations of the whole system are running in the programme code, some internal variables and counters will be established, and their initial conditions are set. Then, the initialisation and configurations of the Firebase database are carried out.

Once the setup is completed, the system will start its operation by obtaining the real-time data from the IMU sensor continuously with the interval of one second. The data obtained will be synchronised into the Firebase real-time database, and the Android application will display the data retrieved from the database. The data shown in the Android application is updated as soon as changes of data in the database are detected. All the processes are performed in an infinite loop. The infinite loop will be interrupted only if there is an input detected by the capacitive touch sensor. The output of the system can be triggered in three ways:

(i) the duration of the input signal on the capacitive touch sensor exceeds five seconds.

(ii) the changes in the acceleration, orientation and temperature meet the thresholds and are maintained for more than 30 seconds.

(iii) speech input matches with the pre-set text.

All three triggering methods are given the same priority. However, as long as any of the triggering methods is fulfilled, the other activation channels of the system will be blocked since they are performing towards the same outcomes. While for the infinite loop, its cycle will be continued if no input is detected by the capacitive touch sensor. Once the system is triggered, the buzzer will be turned on to function as an alarm. Then, the data from the GPS tracking module will be collected and uploaded into the Firebase database. An emergency message will be sent to the pre-set emergency contacts. To ease the monitoring and controlling of the system, the Android application will display all the data obtained throughout the process cycle, and a function of getting the nearest safe location can be activated in the Android application. The speech

recognition and automatic alarm functions can also be switched off through the Android application, and the alarm can be independently controlled in the Android application.

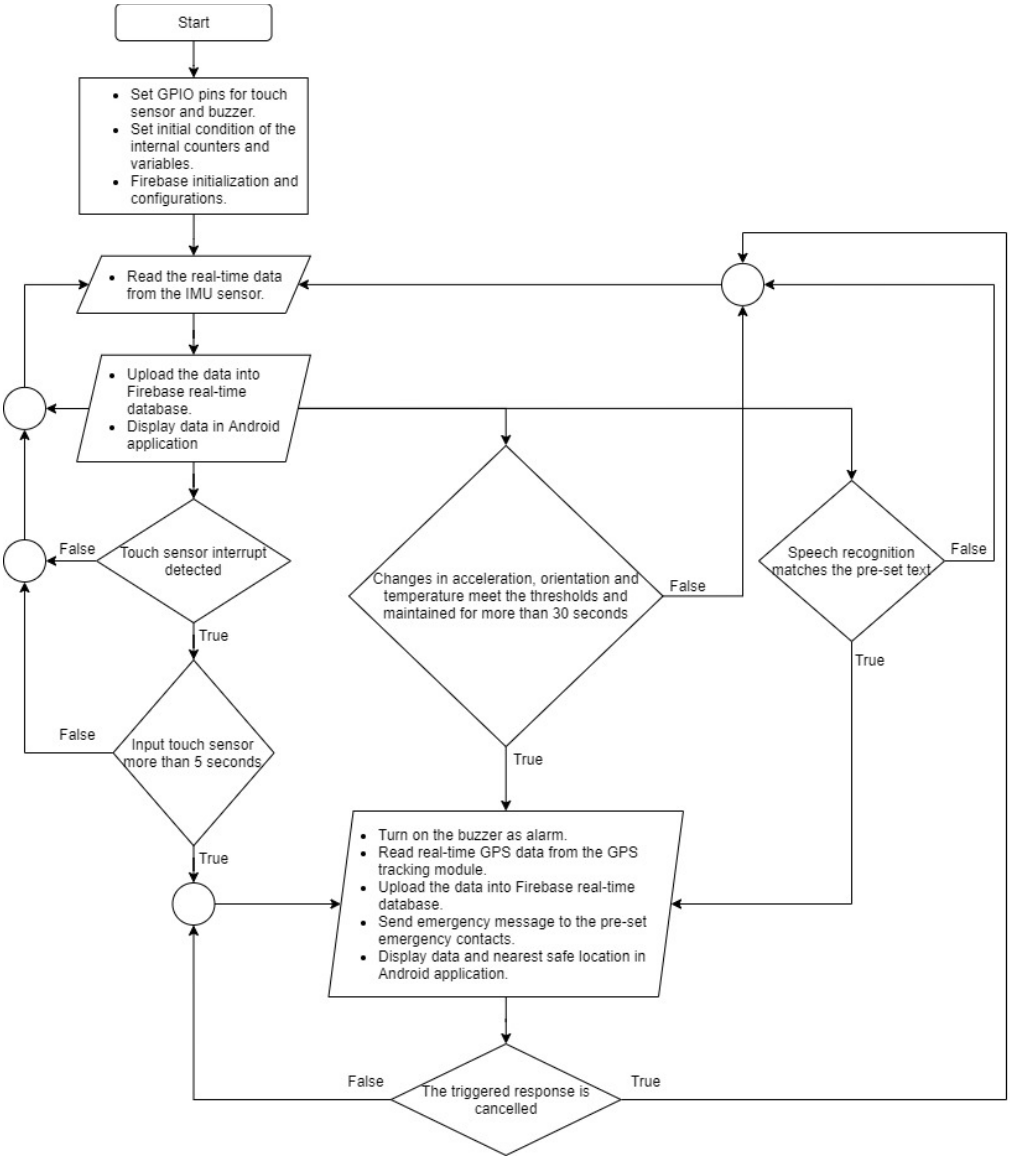


Figure 3.16: The overall flowchart of the system.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

In this section, the results of the project will be discussed with all necessary details provided to prove its accuracy and validity.

4.2 Circuit Design and Pin Connections

The complete circuit connections of the protection system are shown in Figures 4.1 and 4.2. The circuit is drawn and illustrated by using Fritzing software. The Raspberry Pi 3 Model B+ that acts as the main controller in the system will be powered up by a 20000 mAh power bank through the micro USB port. Besides, an external 5 V power supply will be connected to the SIM800L GSM module. The reason that the GSM module is supplied by an external power source instead of using the 5 V supply from the Raspberry Pi 3 Model B+ is to increase the stability of the performance as it is sending and receiving data continuously. If it is powered up by the 5 V pin of the Raspberry Pi 3 Model B+, the maximum baud rate may not be achieved, causing slower transmission of data. Also, there is a reset function in the GSM module, where it will continuously turn on and off if the power supply is unstable. Since there is only one set of UART pins on the Raspberry Pi 3 Model B+, a CH340G USB to TTL Converter Module is applied to convert the USB port into another set of UART pins. The transmit (TX) pin of the GPS tracking module is linked to the receive (RX) pin of the USB to TTL Converter Module so that the GPS tracking module can transmit the data collected and the converter module can receive the data sent. Moreover, the USB Omnidirectional Microphone is connected to and powered by the USB port of the Raspberry Pi 3 Model B+. The detailed pin and port connections of every module are summarised in Table 4.1.

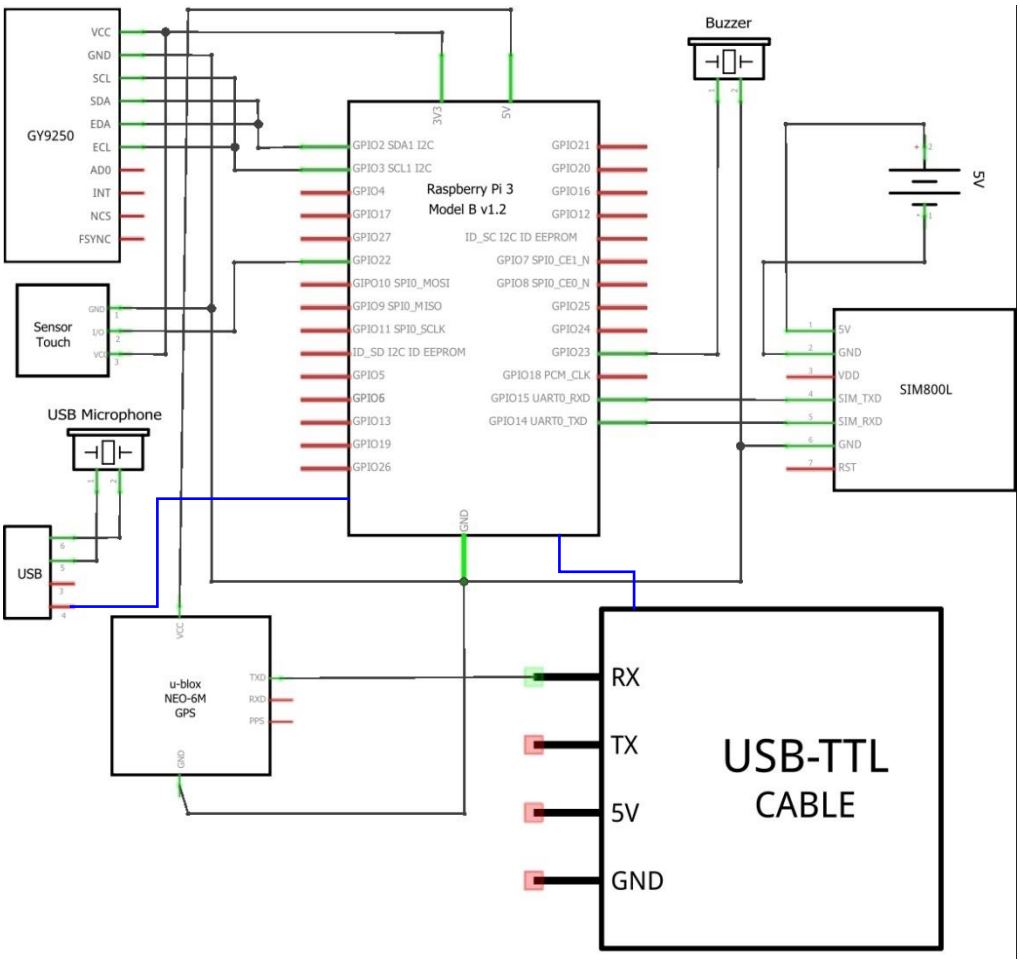


Figure 4.1: The schematic diagram of the circuit design.

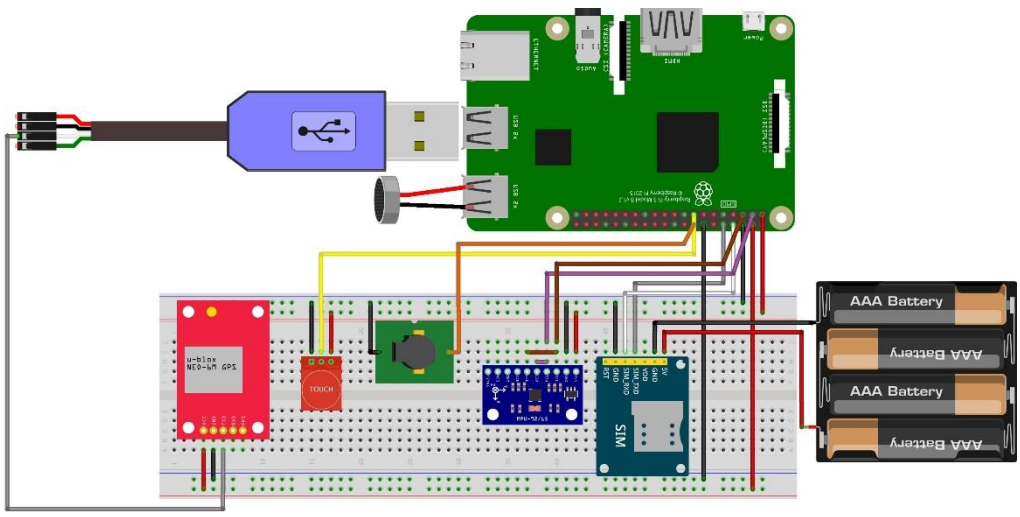


Figure 4.2: The wiring diagram of the circuit design

Table 4.1: Summary of the pin and port connections of the entire system.

Modules	**Modules' Pins and Ports**	**Raspberry Pi's Pins and Ports**
CH340G USB to TTL Converter Module	USB RX	USB TX (GPS module)
TTP223 Capacitive Touch Sensor	VCC GND SIG	3V3 Ground GPIO 22
USB Omnidirectional Microphone	USB	USB
MPU9250 9-axis IMU Sensor	VCC GND SCL SDA EDA ECL	3V3 Ground SCL1 SDA1 SDA1 SCL1
Buzzer	VCC GND	GPIO 23 Ground
GY-NEO6MV2 GPS Tracking Module	VCC GND TX	5V Ground RX (USB to TTL module)
SIM800L GSM Module	5V GND TX RX GND	5V (external power) Ground (external power) RX TX Ground

4.3 Project Prototype

Figure 4.3 shows the final prototype of the IoT based personal safety and protection system. It is temporarily attached to an acrylic board to ease the handling during the experiments.

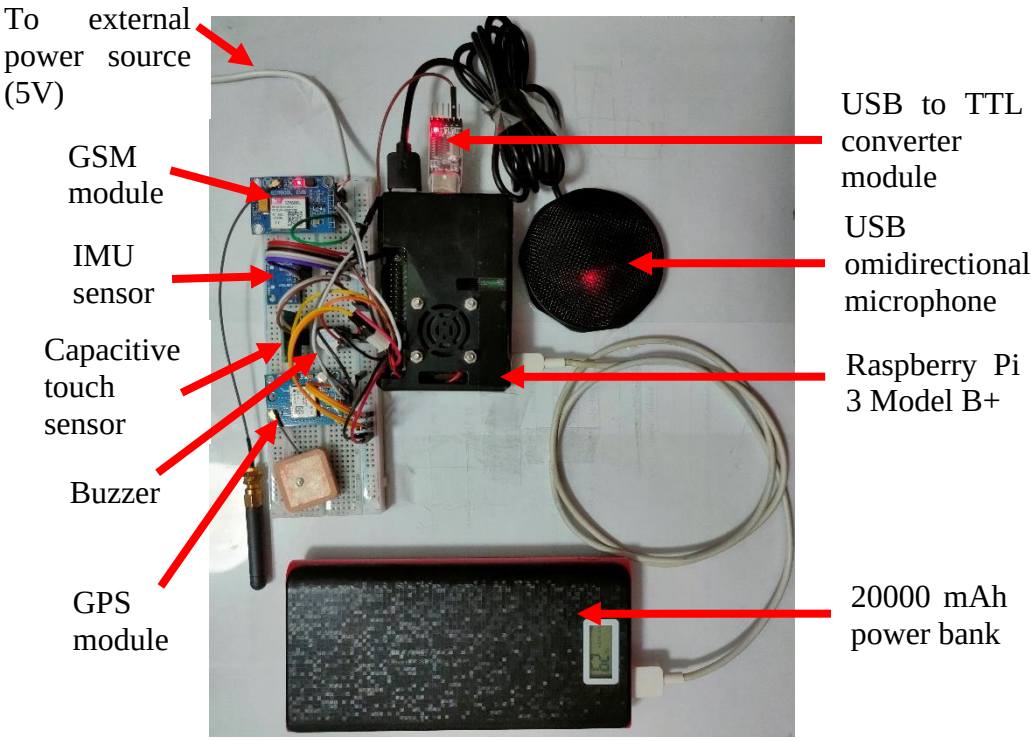


Figure 4.3: The final prototype of the project.

4.4 System Features

Various features of the system are discussed in this section.

4.4.1 Firebase Real-time Database

Figure 4.4 shows part of the data stored in the Firebase real-time database. Nested loops are created to separate the data from each sensor. Those data in the loops of "1-set" is updated in real-time as long as the device is running. On the other hand, the loops labelled "2-push" store the historical data for future data analysis. The "alarm", "count", and "mpu" loops are specially prepared for the toggle buttons in the Android application, where "0" means OFF and "1" indicates ON. These data will then be retrieved by the main programme to determine the user's selection. All the data is stored in the JavaScript Object Notation (JSON) format, which will ease the development of other GUI, such

as web applications. This is due to the data in JSON format can be acquired easily in JavaScript programming language that is widely used in designing the user interface.

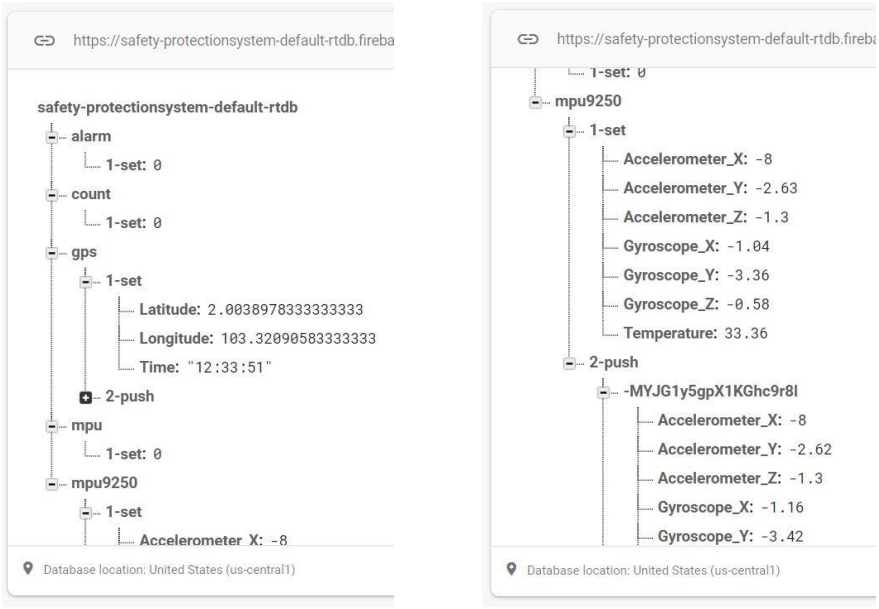


Figure 4.4: Part of the data stored in the Firebase real-time database.

4.4.2 Real-time Monitoring

The data can be monitored by two different methods, which are via the Firebase real-time database as mentioned earlier, and via the Android application on a mobile phone. Figure 4.5 shows the layout of the Android application developed.

Figure 4.5: The Android application layout.

The Android application acts as a more user-friendly interface, in which the user can view the real-time data from the sensors as long as the mobile phone is connected to the internet, regardless of a Wi-Fi network or a cellular network. The application is designed in the way that it will respond to any changes on the data stored in the Firebase real-time database, and immediately retrieve the new, updated information to be displayed on the interface. Furthermore, the Android application can be installed by anyone with the Android application package (APK) file. There are not restricted criteria set for entering the application, and the number of phones that can download the application is not limited. This enables multiple users to monitor the system simultaneously anywhere and anytime even though the device is not placed close to the mobile phone. This adds an advantage for the device that it can be used as a home safety and protection system instead of just to the target of protecting a personnel. For instance, if the device is placed at home, the parents, who are away from home, can always monitor the situation around their child through the Android application. All the real-time information is synchronized with the system, and the system will be triggered once the thresholds are achieved. In Figures 4.6 and 4.7, it can be seen that both the data in the Firebase real-time database and the Android application are updated concurrently.

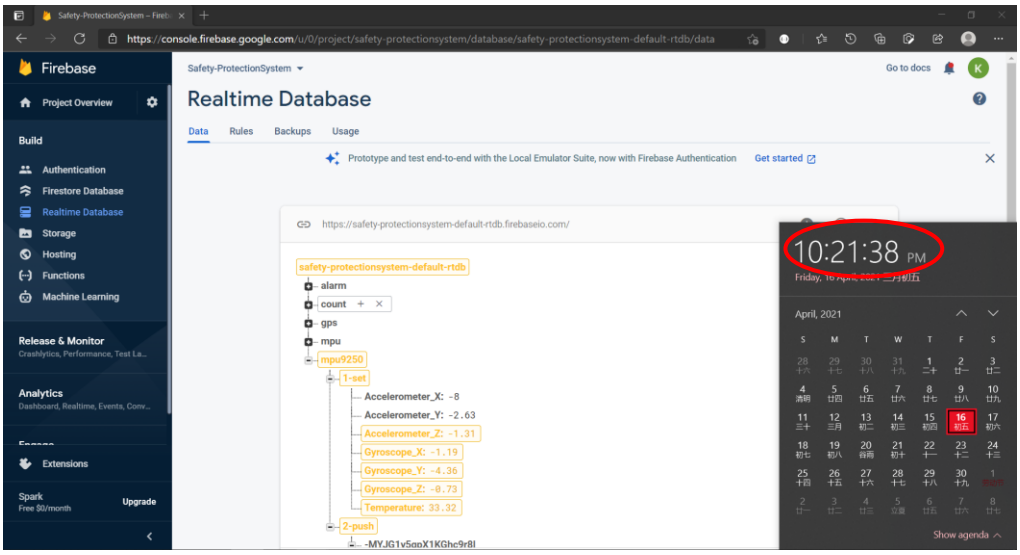


Figure 4.6: The Firebase real-time database with data updating at 10:21:38 p.m.

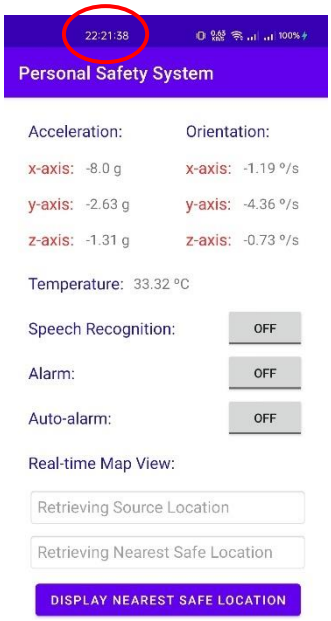


Figure 4.7: The Android application with real-time data at 10:21:38 p.m.

4.4.3 Real-time Controlling

Apart from real-time monitoring, the Android application also provides the function of real-time controlling of the system. This allows the user to customise the safety device according to his usage and requirement. For example, one of the triggering methods of the system is to apply changes to the acceleration and orientation non-stop for more than 30 seconds. Running action perfectly matches with the criteria, in which the acceleration detected will increase with the running speed and the orientation of the user will vary

with the exercising motion. This may cause a false alarm to be activated. The scene of putting the device inside a bag may also trigger the system to output a false alarm because the vibration generated while the user is moving will change the orientation of the device. Therefore, the user can select to turn off the automatic alarm of the system by toggling the button from ON state to OFF state. The same goes for the speech recognition and alarm features. When the speech recognition feature is switched on, it may affect the interval of the real-time data being updated into the Firebase real-time database because the system will go into a loop to receive the speech from the user and analyse it. Although the recording duration of each speech is set to be only four seconds, the process of analysing and converting the speech into text will take longer. The condition may get worse if the speech recognition function is turned on all day long but the user has no intention of using it. This will affect the overall performance of the system. While for the alarm, if the button is toggled ON, the buzzer will be powered up continuously. This feature is specially designed for the user to turn on the alarm immediately whenever it is needed without having to wait for any of the three triggering methods. Figures 4.8 and 4.9 show the data updated in the Firebase real-time database once the toggle buttons in the Android application are pressed. The updated data will then be retrieved by the main programme to execute the appropriate function.

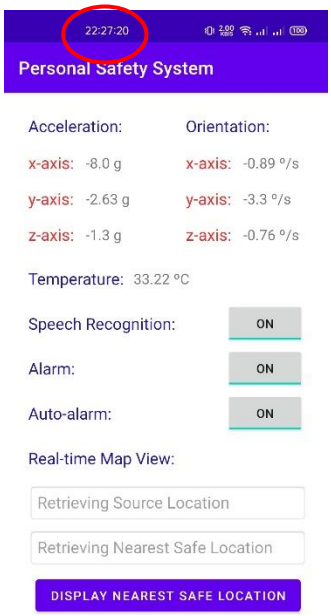


Figure 4.8: The toggle buttons in the Android application are pressed at 10:27:20 p.m.

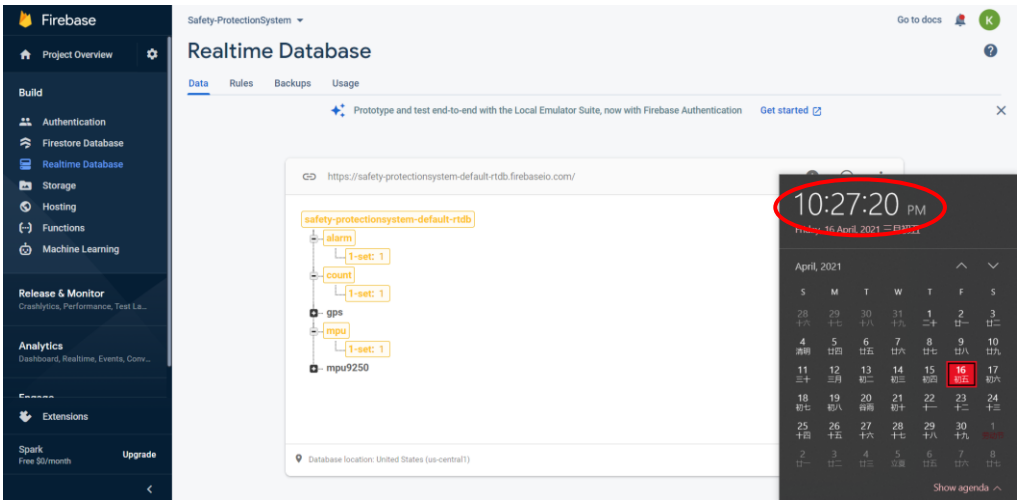


Figure 4.9: The Firebase real-time database with data updating at 10:27:20 p.m.

4.4.4 Real-time Map View

To enhance the safety feature of the system, the real-time map view is included in the Android application. This function allows the user to straight away access Google Maps by staying in the same application. During the first-time usage of this function, the Android application will prompt the user to give permission to access the phone's location as shown in Figure 4.10.

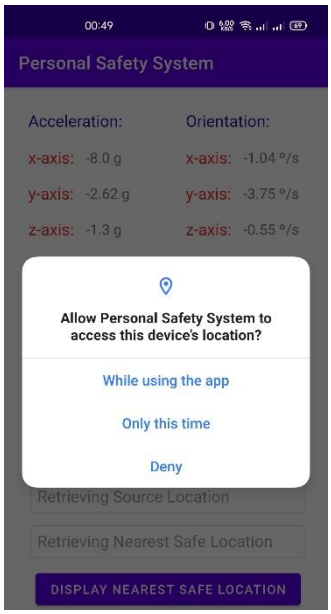


Figure 4.10: The Android application is prompting the user to give permission to access the phone's location during the first-time usage.

Once the permission is approved, the user can use this feature freely in the future. When the button "DISPLAY NEAREST SAFE LOCATION" is pressed, the application will first check for the GPS signal. Pop-up notifications will appear when the phone's GPS is not turned on or has no signal.

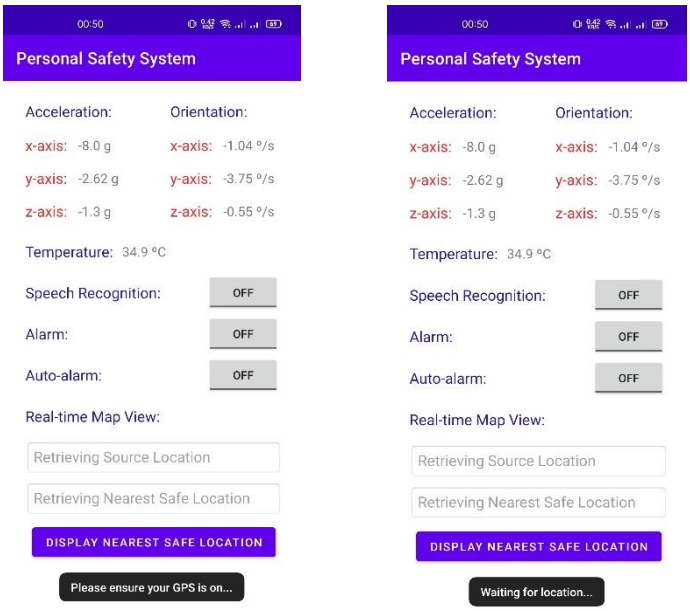


Figure 4.11: Pop-up notifications appear when the GPS of the phone is not turned on or has no signal.

In contrast, if the GPS signal is found, the user will be redirected to Google Maps application to display the track for the nearest safe location, where the source location is predefined as the current location of the phone and the nearest safe location is chosen to be the nearest police station. With these settings, Google Maps will directly search for the route from the user's phone to the closest police station. This is useful in an emergency situation, where the user has no time and chance in typing the words one by one to search for the route. The reason for fixing the source location as the current phone's location instead of the device's location is to avoid the wrong source location obtained when the user is not carrying the phone and the safety device at the same time. It also offers a precautionary step in the case where the user accidentally drops the safety device in a dangerous event. Generally, a person will choose to wear his/her phone in the pants' or trousers' pocket. Thus, it can be confirmed that the chance of a phone being dropped will definitely be much lower than that of the safety device which is normally placed inside a bag. Even if the phone is lost, the user will be unreachable to the Android application. There is no point to set the source location to be the safety device's location.

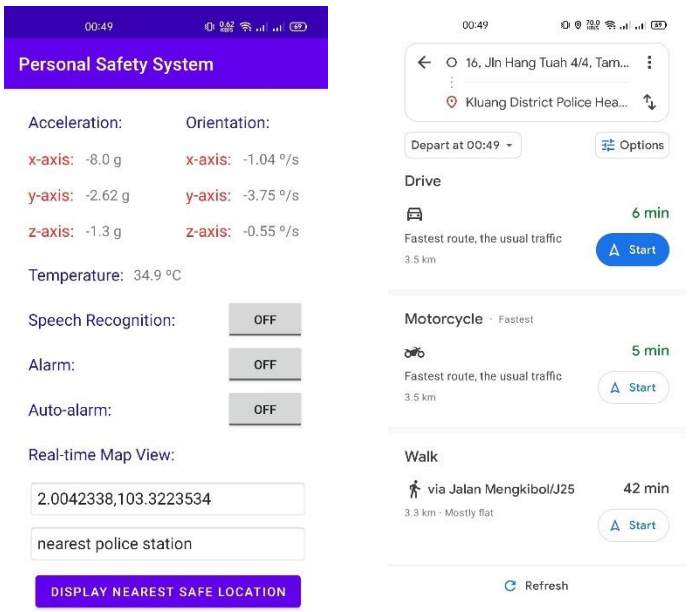


Figure 4.12: The application will redirect the user to Google Maps after pressing the button.

4.4.5 Real-time Notification

An additional safety feature of real-time notification is implemented to notice the emergency contacts predefined in the system that the user is facing a dangerous situation. It acts as an external communication channel, which automatically links the user to the external source of help to request urgent assistance. Whenever the system is activated, this feature will be called by the main programme and it works instantly regardless of which triggering methods. The SMS will then be spontaneously sent to the emergency contacts through the subscriber identification module (SIM) card inserted in the GSM module. The SMS content is as shown in Figure 4.13, where the emergency message is followed by the latitude and longitude of the safety device as well as a web page link that will direct the reader to the Google Maps view of the latitude and longitude. With that, the track from the emergency contacts to the user who is in a dangerous situation can be obtained quickly. The emergency contacts can perform immediate action to log a police report and search for the user to reduce the possibility of victimisation. This feature will be continuously executed until the user has triggered to stop the system.

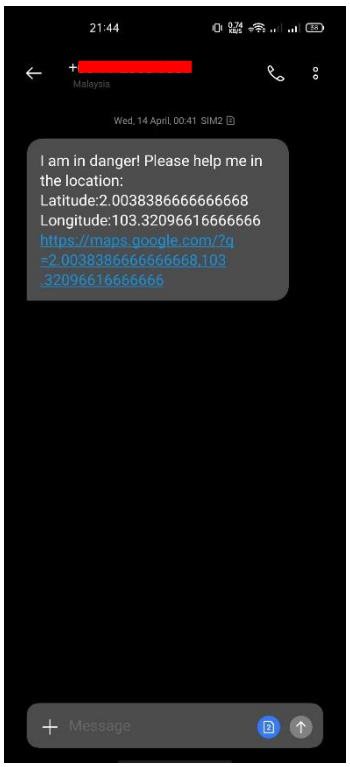


Figure 4.13: The real-time notification sent to the pre-set emergency contacts in the form of SMS.

4.5 Experiment

Various experiments are carried out to validate the functionality and the performance of the prototype. The threshold values for triggering the system automatic alarm are also fixed through the experiments.

4.5.1 Threshold Settings

The threshold values of the acceleration and orientation are selected based on the results obtained from multiple times of various experiments, such as mock running and falling tests by three participants, as well as temperature tests under four conditions, which are indoor, outdoor, indoor with fire, and outdoor with fire. The orientation is determined in terms of the angular velocity measured by the IMU sensor. Since the sensor outputs the acceleration in the unit g and angular velocity in the unit °/s, some conversions are required to be done to transform the results into the International System of Units (SI) to ease the data analysis for future improvement. For the acceleration, its SI unit is m/s^2, but the data obtained from the sensor is in g. Conversion can be done by substituting the formula of g = 9.81 m/s^2 into the data, in which each acceleration result is multiplied with 9.81 m/s^2 to get them in the SI unit. While for the angular velocity, its SI unit is rad/s, but the data obtained from the sensor is in °/s. It is known that 1° = π/180 rad. By multiplying every angular velocity result with π/180 rad, the data in the SI unit can be calculated. The results of all experiments are shown in Tables 4.3, 4.4, and 4.5. In this discussion, the x-axis is set to be the directions in front and behind the user, the y-axis is the right and left directions of the user, and the z-axis is the up and down directions of the user.

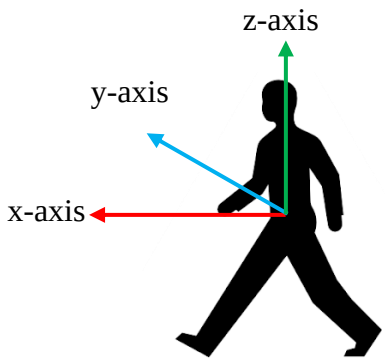


Figure 4.14: The axes settings in this discussion.

From the results of the mock falling experiments in Table 4.3, it is found that only the z-axis acceleration experiences some obvious changes, and there are large effects on the angular velocity. Try to imagine the motion that happens when a person falls down. Since the person is moving downwards, there is no significant acceleration change in both the x-axis and y-axis. Yet, during the falling, the angular velocity will be increased as there is a rotational motion happening to the user. By assuming the starting point of the rotation is along the z-axis, after the falling action, the ending point should locate along the x-axis. Therefore, greater changes in the angular velocity are detected during the mock falling tests. On the other hand, when a running action is carried out by a person, both acceleration and angular velocity will undergo large changes. This is due to the device is being vibrated heavily and it is very hard to predict the actual running motion of the user by just looking at the acceleration and angular velocity. From the results obtained, it is found that the values will vary with the falling and running habits of the user. Thus, the thresholds to trigger the system are determined by taking the suitable range between the data obtained when there is neither falling nor running action and the highest or lowest amplitude in the data acquired during the falling and running action. While for the temperature, the value of 45 ºC is chosen to be the threshold since the normal temperature level in Malaysia is around 32 ºC to 40 ºC. In this project, the thresholds set are as follow:

(i) Acceleration in the z-axis: greater than 0.5 g.

(ii) Angular velocity in the x-axis: smaller than -2 º/s or greater than 5 º/s.

(iii) Angular velocity in the y-axis: smaller than -6 º/s or greater than -2 º/s.

(iv) Angular velocity in the z-axis: smaller than -1 º/s or greater than -0.2 º/s.

(v) Temperature: greater than 45 ºC.

Table 4.2: The data obtained under normal conditions.

Acceleration (g)			**Angular Velocity (º/s)**			**Temperature (ºC)**
x-axis	y-axis	z-axis	x-axis	y-axis	z-axis	
-8.00	-2.62	-1.31	-0.89	-4.03	-0.31	31.94

Table 4.3: Mock falling experiments by participants A, B, and C.

Time (s)	**Acceleration (g)**									**Angular Velocity (º/s)**								
	x-axis			y-axis			z-axis			x-axis			y-axis			z-axis		
	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
1	-8.00	-8.00	-8.00	-2.64	-2.64	-2.63	-1.29	-1.29	-1.30	-0.82	-0.79	-0.98	-0.95	-3.17	-3.45	3.11	-0.55	-0.79
2	-8.00	-8.00	-8.00	-2.71	-2.65	-2.64	-1.32	-1.31	-1.29	-2.84	-1.53	28.72	-10.28	-0.92	-87.86	-0.21	-0.7	2.53
3	-8.00	-8.00	-8.00	-2.68	-2.65	-3.39	-0.09	-0.01	-0.50	19.07	-28.02	-0.76	-69.85	41.20	-4.00	10.96	2.47	-0.09
4	-8.00	-8.00	-8.00	-2.67	-2.65	-3.38	0.68	-0.21	-0.49	-9.86	-3.66	-1.65	68.30	-5.07	-8.76	8.91	-0.52	0.58
5	-8.00	-8.00	-8.00	-2.67	-2.65	-3.38	0.74	-0.25	-0.49	-3.6	-2.04	0.21	-3.20	-5.22	-4.73	-1.65	-0.79	0.82
6	-8.00	-8.00	-8.00	-2.73	-2.65	-3.37	0.70	-0.28	-0.48	5.89	-1.59	-0.15	2.62	-4.43	-3.94	0.76	-0.55	0.37
7	-8.00	-8.00	-8.00	-2.70	-2.65	-3.33	0.69	-0.37	-0.58	-1.83	1.50	-24.90	-4.12	-9.03	6.56	0.37	-0.49	15.50
8	-8.00	-8.00	-8.00	-2.84	-2.65	-2.65	-1.21	-0.42	-1.29	-20.14	0.27	-2.93	-9.06	-7.35	-0.85	-13.73	-0.76	-0.61
9	-8.00	-8.00	-8.00	-2.65	-2.62	-2.78	-1.29	-1.29	-1.31	-1.53	-1.28	18.16	-4.15	-4.12	26.79	-0.67	-1.95	2.04
10	-8.00	-8.00	-8.00	-2.64	-2.63	-2.64	-1.32	-1.3	-1.30	-1.16	-0.73	-1.13	-2.69	-3.27	-3.48	-0.31	-0.67	-0.61

Table 4.4: Mock running experiments by participants A, B, and C.

Time (s)	**Acceleration (g)**									**Angular Velocity (º/s)**								
	x-axis			y-axis			z-axis			x-axis			y-axis			z-axis		
	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
1	-8.00	-8.00	-8.00	-2.63	-2.64	-2.58	-1.32	-1.32	-0.77	-3.33	-6.13	-6.68	0.12	6.41	-14.56	6.01	1.07	18.65
2	-8.00	-8.00	-8.00	-3.03	-2.65	-2.54	-2.01	-1.35	-1.49	-7.23	-24.26	-30.79	95.00	-65.28	-21.76	-87.68	-70.22	47.67
3	-8.00	-8.00	-8.00	-3.05	-2.65	-2.45	-1.42	-1.74	-1.21	1.83	-11.38	28.47	-47.00	109.41	60.30	99.82	8.00	-22.86
4	-8.00	-8.00	-8.00	-3.16	-3.25	-2.64	-1.62	-1.58	-1.84	28.63	19.35	29.91	-157.17	-45.01	112.34	164.12	-44.19	-62.19
5	-8.00	-8.00	-8.00	-2.88	-3.23	-2.73	-1.37	-0.72	-1.18	-18.74	-10.13	-7.39	-72.54	-58.29	63.66	-10.77	70.37	48.19
6	-8.00	-8.00	-8.00	-2.74	-3.18	-3.09	-0.50	-1.70	-1.79	2.35	53.99	-19.78	-15.20	45.36	66.71	-4.82	-50.17	-69.52
7	-8.00	-8.00	-8.00	-2.86	-3.19	-2.30	0.27	-0.90	-1.40	-3.48	-10.59	-16.63	-20.39	-79.65	21.10	-3.05	25.82	-19.53
8	-8.00	-8.00	-8.00	-2.79	-3.20	-2.60	0.57	-1.95	-1.21	-10.28	12.60	9.49	-10.10	-2.87	-24.23	-3.97	-21.82	152.89
9	-8.00	-8.00	-8.00	-2.79	-2.89	-3.21	0.64	-1.08	-1.36	2.14	41.35	-0.52	-6.59	-11.84	0.73	0.61	0.31	-18.62
10	-8.00	-8.00	-8.00	-2.65	-2.90	-3.13	-1.32	-1.31	-1.12	-4.58	-0.92	-1.25	0.37	-4.61	-38.33	-0.89	-0.43	72.14

Table 4.5: Temperature tests on various conditions.

Conditions	**Temperature (°C)**					
	Test 1	Test 2	Test 3	Test 4	Test 5	Average
Indoor	32.26	32.45	31.93	32.17	32.45	32.25
Outdoor	35.56	35.29	35.37	35.68	35.44	35.47
Indoor with fire	84.48	84.37	84.43	84.45	84.39	84.42
Outdoor with fire	84.26	82.01	85.07	83.78	82.34	83.49

4.5.2 Power Consumption

Since the whole system is powered by a 20000 mAh power bank, the power consumption of the prototype may become one of the criteria that the user concerns about. Table 4.6 shows the results obtained from the experiment to test the power consumption. According to RasPi.TV (2018), a Raspberry Pi 3 Model B+ consumes about 520 mAh while shooting 1080p video. The electrical power required is calculated to be 0.52 A × 5 V = 2.6 W. As the mAh rating of a power bank refers to its nominal cell voltage, which is 3.7 V for a typical lithium-ion based power bank, and not to its output voltage of 5 V, a 20000 mAh power bank has a capacity of about 20 Ah × 3.7 V = 74 Wh. Thus, the expected running time of the Raspberry Pi when powered by a 20000 mAh power bank with full capacity is 74 Wh / 2.6 W = 28.5 h. However, the actual runtime will highly depend on many unpredictable aspects like CPU usage, Wi-Fi usage, connected hardware, etc. So, it is assumed that the theoretical actual runtime will be around 50 % of the expected runtime, which is 28.5 h / 2 = 14.25 h. From the experiment, the power bank is only capable of supplying power to the Raspberry Pi 3 Model B+ for about nine hours. This may be due to two main reasons. Firstly, the system is continuously running the main programme in an infinite loop and the process of retrieving and synchronising data into the Firebase database is non-stop. Besides, the power bank may have already degraded to contain less than 20000 mAh since it is not newly purchased. Anyway, since it is just a prototype, the duration of nine hours is enough for common usage. The battery can be upgraded when the system is going to be manufactured on a large scale.

Table 4.6: The power consumption of the prototype.

Time (h)	**Battery Level (%)**
0	100
1	89
2	78
3	67
4	56
5	45
6	34
7	23
8	12
9	0

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

An IoT based personal safety and protection system has been successfully developed in this project. It is a more reliable design than those conventional personal safety systems available in the market due to its capability of protecting and supporting the user during an emergency with three different triggering methods:

(i) the duration of the input signal on the capacitive touch sensor exceeds five seconds.

(ii) the changes in the acceleration, orientation and temperature meet the thresholds and are maintained for more than 30 seconds.

(iii) speech input matches with the pre-set text.

All these activation methods are designed in a way to avoid the false alarm problem in the conventional devices that will affect the overall performance of the system. Besides, the developed system features the function of synchronising the real-time data obtained from the sensors into cloud storage. The data stored can then be analysed to investigate the performance of the system and improvement can be applied to enhance the specifications of the system in the future. In order to establish a more user-friendly design and service, the personal safety and protection system developed comes with an Android application that is capable of providing real-time monitoring and controlling functions to realise the remote communication between the user and the device. Personalisation of the system can be done by the user to amend the system according to his needs and usage.

During the process of customisation, the Android application communicates with the safety device through the cloud server by modifying the data stored in the real-time database. The whole process is very fast and precise, which further increases the reliability of the system. An additional

real-time map view is appended in the Android application to further enrich the safety features of the system. To prove the accuracy and precision of the system performance, various experiments have been executed multiple times to study the efficiency and effectiveness of the entire system. In conclusion, it can be said that the personal safety and protection system developed in this project is one of the best in the current market, and it is dependable to guarantee the user's safety. All the aim and objectives have been achieved.

5.2 Recommendations for Future Work

Several recommendations can be done for future work to overcome the limitations and improve the overall performance as well as features of the system developed. Firstly, the size of the prototype can be minimised by migrating all the hardware into an integrated circuit design. In this project, since the hardware is bought and installed separately for testing, the prototype is large and heavy for convenient usage. In the future, a PCB can be designed to fit all the hardware in a small circuit board to reduce the weight and size of the device. Next, due to the budget problem, the battery used in this project is a 20000 mAh power bank that is huge. In future work, it is recommended that the power bank can be replaced by a built-in lithium-ion battery similar to a phone battery to provide better endurance to the idling mode of the device and extend the battery life.

Thirdly, one of the limitations of this project is that the cloud server only permits storage of 20000 data per day for the free version. If the system developed is going to be used for 24 hours per day, there will be insufficient data storage, leading to failure of the entire system. In future work, if the system developed is going to be manufactured on a large scale, subscription to the cloud server can be done to solve this problem easily as it is more cost-effective when the subscription fee is divided into the production cost of each device. Lastly, the data collected in cloud storage can be utilised to perform machine learning to study the motion generated according to the user's habits. Through the result of machine learning, the thresholds can be determined more scientifically.

REFERENCES

Ahir, S., Kapadia, S., Chauhan, J., and Sanghavi, N., 2018. The personal stun - A smart device for women's safety. *International Conference on Smart City and Emerging Technology (ICSCET)*, [e-journal]. https://doi.org/10.1109/ICSCET.2018.8537376

American District Telegraph (ADT), n.d. *Our history*. [online] Available at: <https://www.adt.com/about-adt/history#:~:text=1874%E2%80%931890&text=American%20District%20Telegraph%20(ADT)%20Founder,first%20residential%20security%20system%20network.> [Accessed 10 July 2020].

Bankar, S. A., Basatwar, K., Divekar, P., Sinha, P., and Gupta, H., 2018. Foot device for women security. *Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018)*, [e-journal] 345–347. https://doi.org/10.1109/ICCONS.2018.8662947

Batra, A., 2008. Foreign tourists' perception towards personal safety and potential crime while visiting Bangkok. *International Journal of Tourism and Hospitality Research*, [e-journal] 19(1), 89–101. https://doi.org/10.1080/13032917.2008.9687055

Bhawana, D., and Neetu, S., 2014. Crimes against women and societal ills: An overview. *International Journal of Advanced Scientific and Technical Research*, [e-journal] 3(4), 44–56. Available at: <http://www.rspublication.com/ijst/index.html> [Accessed 20 July 2020].

Cytron Technologies, n.d. *Raspberry Pi 3 Model B+*. [online] Available at: <https://my.cytron.io/p-raspberry-pi-3-model-b-plus?src=account.order> [Accessed 5 September 2020].

Department of Statistics, Malaysia, 2019. *Crime statistics, 2019*. [online] Available at: <https://www.dosm.gov.my/v1/index.php/index.php?r=column/cthemeByCat&cat=455&bul_id=MEs4QzNxWkNZZDEyM08yM0Jsd05vQT09&menu_id=U3VPMldoYUxzVzFaYmNkWXZteGduZz09#:~:text=Crime%20index%20ratio%20per%20100%2C000,level%20in%202018%20namely%20W.P.&text=Meanwhile%2C%20Terengganu%20recorded%20the%20lowest,index%20for%202018%20(148.4).> [Accessed 10 July 2020].

Desai, N., Dhameliya, K., and Desai, V., 2013. Feature extraction and classification techniques for speech recognition: A review. *International Journal of Emerging Technology and Advanced Engineering*, [e-journal] 3(12), 367-371. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.433.7519&rep=rep1&type=pdf> [Accessed 20 July 2020].

Google Developers, n.d. *Brand guidelines: Representing the Firebase brand*. [online] Available at: <https://firebase.google.com/brand-guidelines> [Accessed 12 September 2020].

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Human Rights Commission of Malaysia (SUHAKAM), 2010. *SUHAKAM's report: The status of women's rights in Malaysia.* [e-book] Malaysia: Human Rights Commission of Malaysia. Available at: <http://www.suhakam.org.my/wp-content/uploads/2013/11/SUHAKAM-Report-on-The-Status-of-Women-s-Rights-in-Malaysia-2010.pdf> [Accessed 20 July 2020].

Iancu, B., 2019. Evaluating Google Speech-to-Text API's performance for Romanian e-learning resources. *Informatica Economică*, [e-journal] 23(1), 17-25. https://doi.org/10.12948/issn14531305/23.1.2019.02

Karpagavalli, S., and Chandra, E. H., 2016. A review on automatic speech recognition architecture and approaches. *International Journal of Signal Processing*, [e-journal] 9(4), 393-404. https://doi.org/10.14257/ijsip.2016.9.4.34

Khan, R., Khan, S. U., Zaheer, R., and Khan, S., 2012. Future internet: The Internet of Things architecture, possible applications and key challenges. *Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12)*, [e-journal] 257–260. https://doi.org/10.1109/FIT.2012.53

Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., and Agrawal, D. P., 2015. Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, [e-journal] 28, 68–90. https://doi.org/10.1016/j.adhoc.2014.12.006

Monisha, D.G., Monisha, M., Pavithra, G., and Subhashini, R., 2016. Women safety device and application - FEMME. *Indian Journal of Science and Technology*, [e-journal] 9(10). https://doi.org/10.17485/ijst/2016/v9i10/88898

Overseas Security Advisory Council, Bureau of Diplomatic Security, U.S. Department of State, 2020. *Malaysia 2020 crime & safety report*. [online] Available at: <https://www.osac.gov/Country/Malaysia/Content/Detail/Report/148f55ab-9111-47ef-99e4-1811a5d28a20> [Accessed 20 July 2020].

Peña-López, I., 2005. *ITU internet reports 2005: The Internet of Things*. [online] Available at: <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf> [Accessed 30 July 2020].

Raspberry Pi Foundation, n.d. *GPIO*. [online] Available at: <https://www.raspberrypi.org/documentation/usage/gpio/> [Accessed 10 September 2020].

RasPi.TV, 2018. *How much power does Raspberry Pi 3A+ plus use?* [online] Available at: <https://raspi.tv/2018/how-much-power-does-raspberry-pi-3a-plus-use> [Accessed 12 April 2021].

Rohana, S., Zaly, S., and Hairul, N. I., 2013. A dilemma of crime and safety issues among vulnerable travellers in malaysian urban environment. *Procedia - Social and Behavioral Sciences*, [e-journal] 105(2013), 498–505. https://doi.org/10.1016/j.sbspro.2013.11.053

Saad, C., Cheikh, E. A., Mostafa, B., and Abderrahmane, H., 2014. Comparative performance analysis of wireless communication protocols for intelligent sensors and their applications. *International Journal of Advanced Computer Science and Applications (IJACSA)*, [e-journal] 5(4), 76–85. Available at: <https://arxiv.org/ftp/arxiv/papers/1409/1409.6884.pdf> [Accessed 14 August 2020].

Shaikh, N., and Deshmukh, R. R., 2016. Speech recognition system – A review. *IOSR Journal of Computer Engineering*, [e-journal] 18(4), 1-9. https://doi.org/10.9790/0661-1804020109

Sharma, K., and Dhir, N., 2014. A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with comparison. *International Journal of Computer Science and Information Technologies (IJCSIT)*, [e-journal] 5(6), 7810 – 7813. Available at: <https://pdfs.semanticscholar.org/ff3e/8a75932416553f16adf113245c1842a0f09b.pdf> [Accessed 14 August 2020].

Sethi, P., and Sarangi, S. R., 2017. Internet of Things: Architectures, protocols, and applications. *Hindawi Journal of Electrical and Computer Engineering*, [e-journal] 2017. https://doi.org/10.1155/2017/9324035

Sogi, N. R., Chatterjee, P., Nethra, U., and Suma, V., 2018. SMARISA: A Raspberry Pi based smart ring for women safety using IoT. *International Conference on Inventive Research in Computing Applications (ICIRCA)*, [e-journal] 451–454. https://doi.org/10.1109/ICIRCA.2018.8597424

SSH.com, n.d. *SSH protocol – Secure remote login and file transfer*. [online] Available at: <https://www.ssh.com/academy/ssh/protocol> [Accessed 10 April 2021].

Vahini, S., and Vijaykumar, N., 2017. Efficient tracking for women safety and security using IoT. *International Journal of Advanced Research in Computer Science*, [e-journal] 8(9), 328 – 330. http://dx.doi.org/10.26483/ijarcs.v8i9.4915

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I. S., Mazura, M., Harrison, M., Eisenhauer, M., and Doody, P., 2011. *Internet of things strategic research roadmap. Internet of Things: Global Technological and Societal Trends*, [e-book] River Publishers. Available at: <https://www.researchgate.net/publication/267566519_Internet_of_Things_Strategic_Research_Roadmap> [Accessed 30 July 2020].

Victory, J, 2019. *How loud is too loud?* [online] Available at: <https://www.healthyhearing.com/report/52694-How-loud-is-too-loud> [Accessed 10 April 2021].

Vijaylashmi, B., Renuka, S., Chennur, P., and Patil, S., 2015. Self defense system for women safety with location tracking and SMS alerting through GSM network. *International Journal of Research in Engineering and Technology (IJRET)*, [e-journal] 4(5), 57–60. Available at: <https://ijret.org/volumes/2015v04/i17/IJRET20150417013.pdf> [Accessed 25 July 2020].

APPENDICES

APPENDIX A: Programme Codes

main.py

```
from touch_sensor import*
from MPU9250 import*
from gpsUSB import*
from speech import*
from sms import*
import time
import signal
import sys
import RPi.GPIO as GPIO
import pyrebase #firebase
from datetime import datetime, timedelta
import multiprocessing

TOUCH_GPIO = 22
BUZZER_GPIO = 23

GPIO.setwarnings(False)
GPIO.setmode(GPIO.BCM)
GPIO.setup(TOUCH_GPIO, GPIO.IN, GPIO.PUD_UP)
GPIO.setup(BUZZER_GPIO, GPIO.OUT)

count = 0
special_event = False
record = ''

config = {
    "apiKey": "T6GwpisDOd0sJhv1Qzo49y0QFsAQ2rxAterAg9cC",
    "authDomain": "safety-protectionsystem.firebaseapp.com",
    "databaseURL": "https://safety-protectionsystem-default-
rtdb.firebaseio.com",
    "storageBucket": "safety-protectionsystem.appspot.com"
}

firebase = pyrebase.initialize_app(config)
db = firebase.database()

if __name__ == "__main__":
    GPIO.setwarnings(False)
    GPIO.setmode(GPIO.BCM)

    GPIO.setup(TOUCH_GPIO, GPIO.IN, GPIO.PUD_UP)
```

```
    GPIO.setup(BUZZER_GPIO, GPIO.OUT)
    GPIO.add_event_detect(TOUCH_GPIO, GPIO.BOTH,
        callback=touch_callback, bouncetime=200)

while True:
    dataMPU = obtainMPU()
    print(dataMPU)
    latest_accel_X = dataMPU[0]
    latest_accel_Y = dataMPU[1]
    latest_accel_Z = dataMPU[2]
    latest_gyro_X = dataMPU[3]
    latest_gyro_Y = dataMPU[4]
    latest_gyro_Z = dataMPU[5]
    latest_temperature = dataMPU[6]

    speechRecogON_OFF = db.child("count").child("1-set").get()
    alarmON_OFF = db.child("alarm").child("1-set").get()
    mpuON_OFF = db.child("mpu").child("1-set").get()
    speechRecog = speechRecogON_OFF.val()
    alarm = alarmON_OFF.val()
    mpu = mpuON_OFF.val()

    if speechRecog == 1:
        record = speech_recog()

    if mpu == 0:
        count = 0
        special_event = False
        print(count)

    if ((-
1 < latest_accel_Z or latest_accel_Z > 0.5) or (latest_gyro_X > 5
 or latest_gyro_X < -2) or (latest_gyro_Y < -
6 or latest_gyro_Y > -2) or (latest_gyro_Z < -
1 or latest_gyro_Z > -
0.2) or (latest_temperature > 45)) and count == 0:
        special_event = True
        INTERVAL = timedelta(seconds=5)
        last_checked = datetime.now() - INTERVAL

    if special_event == True and last_checked <= (datetime.now()
- INTERVAL) and ((-
1 < latest_accel_Z or latest_accel_Z > 0.5) or (latest_gyro_X > 5
 or latest_gyro_X < -2) or (latest_gyro_Y < -
6 or latest_gyro_Y > -2) or (latest_gyro_Z < -
1 or latest_gyro_Z > -0.2) or (latest_temperature > 45)):
        count += 1
        INTERVAL = timedelta(seconds=5)
```

```
        last_checked = datetime.now()
        print(count)

    elif special_event == True and last_checked <= (datetime.now(
) - INTERVAL) and not ((-
1 < latest_accel_Z or latest_accel_Z > 0.5) or (latest_gyro_X > 5
 or latest_gyro_X < -2) or (latest_gyro_Y < -
6 or latest_gyro_Y > -2) or (latest_gyro_Z < -
1 or latest_gyro_Z > -0.2) or (latest_temperature > 45)):
        count = 0
        print(count)

    while count > 4 or record == 'help me' or alarm == 1:
        print("enter")
        GPIO.output(BUZZER_GPIO, GPIO.HIGH)
        dataGPS = obtainGPS()
        print(dataGPS)
        sendMessage(dataGPS)

        time.sleep(5)

    if GPIO.input(TOUCH_GPIO):
        record = 'reset'
        count = 0
        print (count)
        special_event == False
        GPIO.output(BUZZER_GPIO, GPIO.LOW)
```

touch_sensor.py

```
import signal
import sys
import time
import RPi.GPIO as GPIO
from gpsUSB import*
from sms import*

TOUCH_GPIO = 22
BUZZER_GPIO = 23

def signal_handler(sig, frame):
    GPIO.cleanup()
    sys.exit(0)

def touch_callback(channel):
    start = time.time()
    elapsed = 0

    while GPIO.input(TOUCH_GPIO):
        GPIO.output(BUZZER_GPIO, GPIO.LOW)
        elapsed = time.time() - start
        print(elapsed)

    while elapsed > 5:
        print("enter")
        GPIO.output(BUZZER_GPIO, GPIO.HIGH)
        dataGPS = obtainGPS()
        print(dataGPS)
        sendMessage(dataGPS)

        if GPIO.input(TOUCH_GPIO):
            GPIO.output(BUZZER_GPIO, GPIO.LOW)
            elapsed = 0
```

MPU9250.py

```
import time
from mpu9250_jmdev.registers import *
from mpu9250_jmdev.mpu_9250 import MPU9250
import pyrebase #firebase
from decimal import Decimal

mpu = MPU9250(
    address_ak=AK8963_ADDRESS,
    address_mpu_master=MPU9050_ADDRESS_68, # In 0x68 Address
    address_mpu_slave=None,
    bus=1,
    gfs=GFS_1000,
    afs=AFS_8G,
    mfs=AK8963_BIT_16,
    mode=AK8963_MODE_C100HZ
)

mpu.configure() # Apply the settings to the registers.

#firebase
config = {
    "apiKey": "T6GwpisDOd0sJhv1Qzo49y0QFsAQ2rxAterAg9cC",
    "authDomain": "safety-protectionsystem.firebaseapp.com",
    "databaseURL": "https://safety-protectionsystem-default-
rtdb.firebaseio.com",
    "storageBucket": "safety-protectionsystem.appspot.com"
}

firebase = pyrebase.initialize_app(config)
db = firebase.database()

def obtainMPU():
    accel = mpu.readAccelerometerMaster()
    gyro = mpu.readGyroscopeMaster()
    temp = mpu.readTemperatureMaster()

    accel_X = round(accel[0],2)
    accel_Y = round(accel[1],2)
    accel_Z = round(accel[2],2)
    gyro_X = round(gyro[0],2)
    gyro_Y = round(gyro[1],2)
    gyro_Z = round(gyro[2],2)
    temperature = round(temp,2)

    dataR = [
        accel_X,
        accel_Y,
```

```
        accel_Z,
        gyro_X,
        gyro_Y,
        gyro_Z,
        temperature
    ]

    data = {
        "Accelerometer_X": accel_X,
        "Accelerometer_Y": accel_Y,
        "Accelerometer_Z": accel_Z,
        "Gyroscope_X": gyro_X,
        "Gyroscope_Y": gyro_Y,
        "Gyroscope_Z": gyro_Z,
        "Temperature": temperature,
    }

    db.child("mpu9250").child("1-set").set(data)
    db.child("mpu9250").child("2-push").push(data)

    time.sleep(1)

    return dataR
```

gpsUSB.py

```
#pyserial library is required for working
import serial
import time
#mport = 'COM9'                      #choose your com port on whic
h you connected your neo 6m GPS
#mport = "/dev/ttyAMA0"               #for Raspberry Pi pins
mport = "/dev/ttyUSB0"              #for Raspberry Pi USB
import pyrebase                      #firebase

ser = serial.Serial(mport,9600,timeout = 2)
config = {
    "apiKey": "T6GwpisDOd0sJhv1Qzo49y0QFsAQ2rxAterAg9cC",
    "authDomain": "safety-protectionsystem.firebaseapp.com",
    "databaseURL": "https://safety-protectionsystem-default-
rtdb.firebaseio.com",
    "storageBucket": "safety-protectionsystem.appspot.com"
}

firebase = pyrebase.initialize_app(config)
db = firebase.database()

def parseGPS(data):
    if data[0:6] == "$GPGGA":
        s = data.split(",")
        if s[7] == '0' or s[7]=='00':
            print ("no satellite data available")
            return

        time = s[1][0:2] + ":" + s[1][2:4] + ":" + s[1][4:6]
        #print("-----------")
        lat = decode(s[2])
        lon = decode(s[4])
        return  time,lat,lon

def decode(coord):
    l = list(coord)
    for i in range(0,len(l)-1):
            if l[i] == "." :
                    break
    base = l[0:i-2]
    degi = l[i-2:i]
    degd = l[i+1:]
    #print(base,"   ",degi,"   ",degd)
    baseint = int("".join(base))
    degiint = int("".join(degi))
    degdint = float("".join(degd))
    degdint = degdint / (10**len(degd))
```

```
    degs = degiint + degdint
    full = float(baseint) + (degs/60)
    #print(full)

    return full

def obtainGPS():
    dataR = []

    while (dataR == []):
        try:
            dat = ser.readline().decode()
            mytime,mylat,mylon = parseGPS(dat)
            #print(mytime,"", mylat, "", mylon)

            dataR = [mytime, mylat, mylon]

            #firebase
            data = {
                "Time": mytime,
                "Latitude": mylat,
                "Longitude": mylon,
            }

            db.child("gps").child("1-set").set(data)
            db.child("gps").child("2-push").push(data)

        except:
            time.sleep(0.1)

    return dataR
```

speech.py

```
import speech_recognition as sr

r = sr.Recognizer()
speech = sr.Microphone(device_index=2)

def speech_recog():
    with speech as source:
        print("say something!…")
        r.adjust_for_ambient_noise(source, duration=1)
        audio = r.listen(source, timeout=4)

        try:
            recog = r.recognize_google(audio, language="en-US")
            recog = 'help me'
            print("You said: " + recog)
            return recog

        except sr.UnknownValueError:
            print("Could not understand audio")

        except sr.RequestError as e:
            print("Could not request results from Google Speech R
ecognition service; {0}".format(e))
```

sms.py

```
import serial
import RPi.GPIO as GPIO
import os, time

GPIO.setmode(GPIO.BCM)

# Enable Serial Communication
port = serial.Serial("/dev/ttyAMA0", baudrate=9600, timeout=1)

# Transmitting AT Commands to the Modem
# '\r\n' indicates the Enter key
def sendMessage(data):
    dataTime = data[0]
    dataLat = data[1]
    dataLong = data[2]

    dataTime = str(dataTime)
    dataLat = str(dataLat)
    dataLong = str(dataLong)

    port.write(('AT'+'\r\n').encode())
    rcv = port.read(15)
    print (rcv)
    time.sleep(1)

    port.write(('ATE0'+'\r\n').encode())      # Disable the Echo
    rcv = port.read(15)
    print (rcv)
    time.sleep(1)

    port.write(('AT+CMGF=1'+'\r\n').encode())  # Select Message f
ormat as Text mode
    rcv = port.read(15)
    print (rcv)
    time.sleep(1)

    port.write(('AT+CNMI=2,1,0,0,0'+'\r\n').encode())   # New SMS
 Message Indications
    rcv = port.read(15)
    print (rcv)
    time.sleep(1)

    # Sending a message to a particular Number
    port.write(('AT+CMGS="+60XXXXXXXXX"'+'\r\n').encode())
    rcv = port.read(15)
    print (rcv)
    time.sleep(1)
```

```
    port.write(('I am in danger! Please help me at the location:'
+'\r\n'+'Latitude: '+dataLat+'\r\n'+'Longitude: '+dataLong+'\r\n'
+'https://maps.google.com/?q='+dataLat+','+dataLong).encode())  #
 Message
    rcv = port.read(15)
    print (rcv)

    port.write(("\x1A").encode()) # Enable to send SMS
    for i in range(10):
        rcv = port.read(15)
        print (rcv)
```

APPENDIX B: Raspberry Pi 3 Model B+ Datasheet

Overview

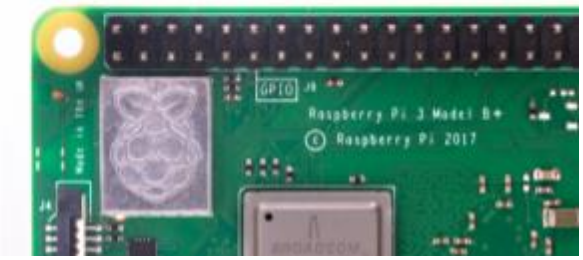
The Raspberry Pi 3 Model B+ is the latest product in the Raspberry Pi 3 range, boasting a 64-bit quad core processor running at 1.4GHz, dual-band 2.4GHz and 5GHz wireless LAN, Bluetooth 4.2/BLE, faster Ethernet, and PoE capability via a separate PoE HAT

The dual-band wireless LAN comes with modular compliance certification, allowing the board to be designed into end products with significantly reduced wireless LAN compliance testing, improving both cost and time to market.

The Raspberry Pi 3 Model B+ maintains the same mechanical footprint as both the Raspberry Pi 2 Model B and the Raspberry Pi 3 Model B.

Specifications

Processor:	Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4GHz
Memory:	1GB LPDDR2 SDRAM
Connectivity:	■ 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE ■ Gigabit Ethernet over USB 2.0 (maximum throughput 300Mbps) ■ 4 × USB 2.0 ports
Access:	Extended 40-pin GPIO header
Video & sound:	■ 1 × full size HDMI ■ MIPI DSI display port ■ MIPI CSI camera port ■ 4 pole stereo output and composite video port
Multimedia:	H.264, MPEG-4 decode (1080p30); H.264 encode (1080p30); OpenGL ES 1.1, 2.0 graphics
SD card support:	Micro SD format for loading operating system and data storage
Input power:	■ 5V/2.5A DC via micro USB connector ■ 5V DC via GPIO header ■ Power over Ethernet (PoE)–enabled (requires separate PoE HAT)
Environment:	Operating temperature, 0–50°C
Compliance:	For a full list of local and regional product approvals, please visit www.raspberrypi.org/products/raspberry-pi-3-model-b+
Production lifetime:	The Raspberry Pi 3 Model B+ will remain in production until at least January 2023.



raspberrypi.org

APPENDIX C: TTP223 Capacitive Touch Sensor Datasheet

Preliminary TTP223

1 KEY TOUCH PAD DETECTOR IC

GENERAL DESCRIPTION

The TTP223 is a touch pad detector IC which offers 1 touch key. The touching detection IC is designed for replacing traditional direct button key with diverse pad size. Low power consumption and wide operating voltage are the contact key features for DC or AC application.

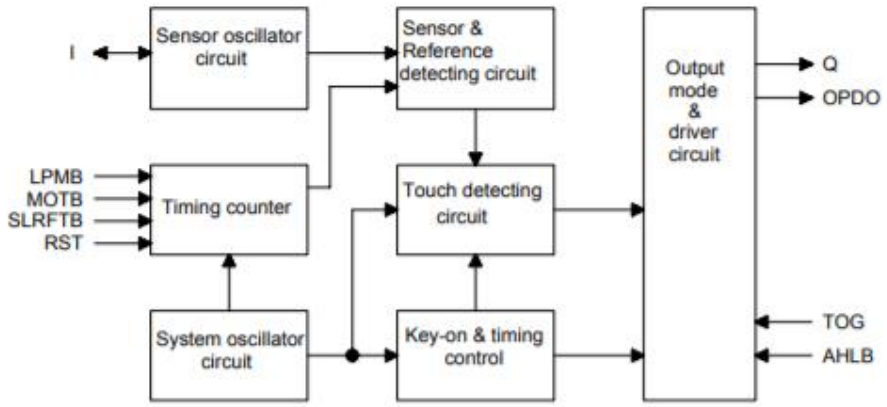
FEATURES

- Operating voltage 2.0V~5.5V
- Operating current @VDD=3V, no load, SLRFTB=1
  At low power mode typical 1.5uA, maximum 3.0uA
  At fast mode typical 3.5uA, maximum 7.0uA
  @VDD=3V, no load, SLRFTB=0
  At low power mode typical 2.0uA, maximum 4.0uA
  At fast mode typical 6.5uA, maximum 13.0uA
- The response time max about 60mS at fast mode, 220mS at low power mode @VDD=3V
- Sensitivity can adjust by the capacitance(0~50pF) outside
- Have two kinds of sampling length by pad option(SLRFTB pin)
- Stable touching detection of human body for replacing traditional direct switch key
- Provides Fast mode and Low Power mode selection by pad option(LPMB pin)
- Provides direct mode、toggle mode by pad option(TOG pin)
  Open drain mode by bonding option, OPDO pin is open drain output,
  Q pin is CMOS output
- All output modes can be selected active high or active low by pad option(AHLB pin)
- Have the maximum on time 100sec by pad option(MOTB pin)
- Have external power on reset pin(RST pin)
- After power-on have about 0.5sec stable-time, during the time do not touch the key pad,
  And the function is disabled
- Auto calibration for life
  And the re-calibration period is about 4.0sec, when key has not be touched

APPLICATION

- Wide consumer products
- Water proofed electric products
- Button key replacement

BLOCK DIAGRAM



PAD DESCRIPTION

Pad No.	Pad Name	I/O Type	Pad Description
1	Q	O	CMOS output pin
2	OPDO	O	Open drain output pin
3	VSS	P	Negative power supply, ground
4	LPMB	I-PH	Low power mode selection, 1=>Fast mode; 0=>Low power mode
5	TOG	I-PL	Output type option pin, 1=>Toggle mode; 0=>Direct mode
6	VDD	P	Positive power supply
7	AHLB	I-PL	Output active high or low selection, 1=>Active low; 0=>Active high
8	RST	I-PL	External power on reset pin
9	SLRFTB	I-PH	Selecting the sampling length, 1=>about 1.6msec; 0=>about 3.2msec
10	MOTB	I-PH	Maximum on time 100sec selection, 1=>Disable, 0=>Enable
11	I	I/O	Input sensor port

ELECTRICAL CHARACTERISTICS

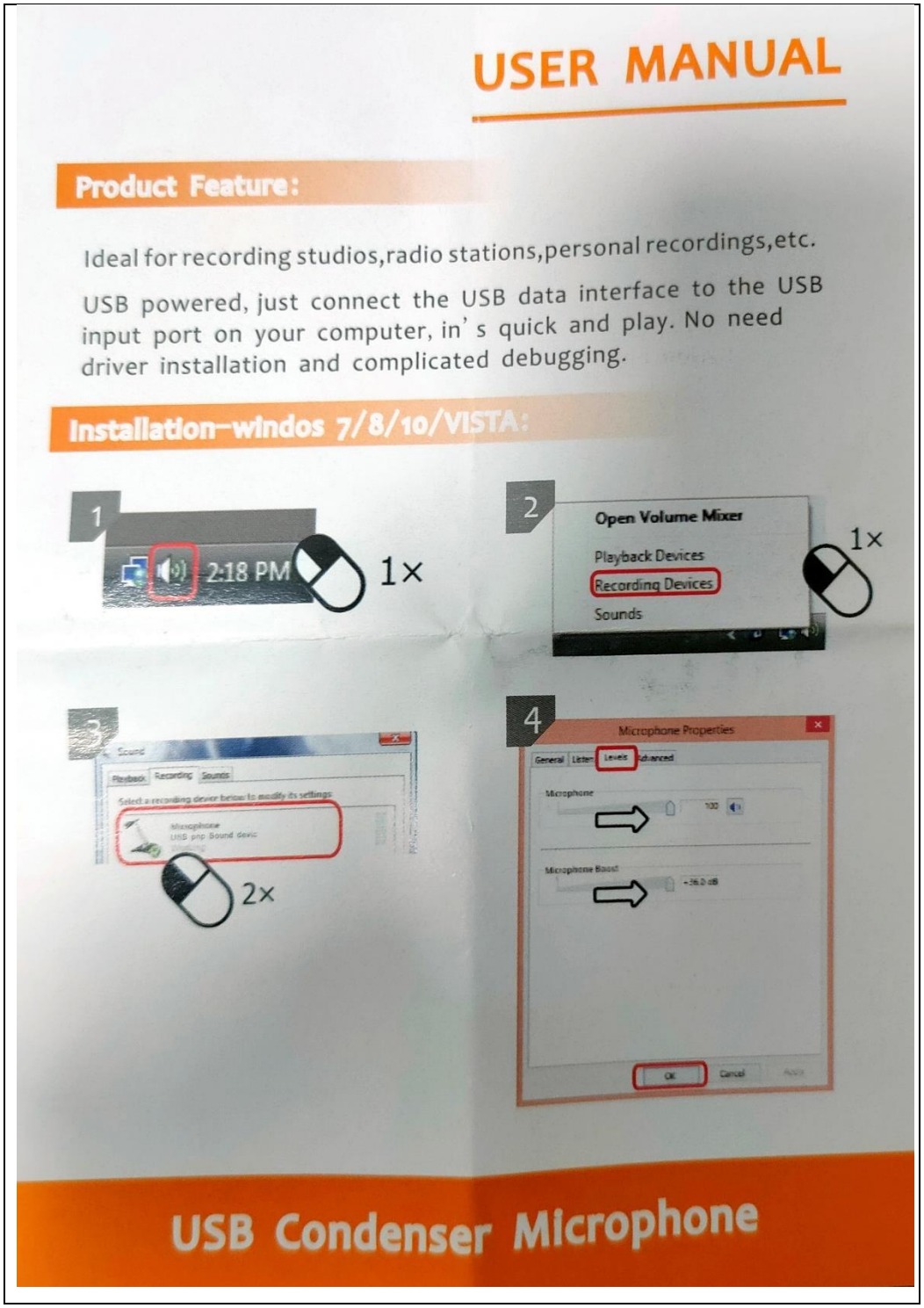
• Absolute Maximum Ratings

Parameter	Symbol	Conditions	Value	Unit
Operating Temperature	T_{OP}	—	-20 ~ +70	℃
Storage Temperature	T_{STG}	—	-50 ~ +125	℃
Power Supply Voltage	VDD	Ta=25°C	VSS-0.3 ~ VSS+5.5	V
Input Voltage	V_{IN}	Ta=25°C	VSS-0.3 ~ VDD+0.3	V
Note：VSS symbolizes for system ground				

• DC/AC Characteristics：(Test condition at room temperature=25℃)

Parameter	Symbol	Test Condition		Min.	Typ.	Max.	Unit
Operating Voltage	VDD			2.0	3	5.5	V
System oscillator	F_{FAST}	VDD=3V		-	512K	-	Hz
	F_{LOW}				16K		
Sensor oscillator	F_{SEN}	VDD=3V no load		-	1M	-	Hz
Operating Current	I_{OP}	VDD=3V at low power mode and output no load	SLRFTB =1	-	1.5	3.0	uA
			SLRFTB =0	-	2.0	4.0	
		VDD=3V at fast mode and output no load	SLRFTB =1	-	3.5	7.0	
			SLRFTB =0		6.5	13.0	
Input Ports	V_{IL}	Input Low Voltage		0	-	0.2	VDD
Input Ports	V_{IH}	Input High Voltage		0.8	-	1.0	VDD
Output Port Sink Current	I_{OL}	VDD=3V, V_{OL}=0.6V		-	8	-	mA
Output Port Source Current	I_{OH}	VDD=3V, V_{OH}=2.4V		-	-4	-	mA
Output Response Time	T_R	VDD=3V, At fast mode				60	mS
		VDD=3V, At low power mode				220	
Input Pin Pull-high Resistor	R_{PH}	VDD=3V, (LPMB, MOTB, SLRFTB)			35K		ohm
Input Pin Pull-low Resistor	R_{PL}	VDD=3V, (TOG, AHLB)			28K		ohm
		VDD=3V, (RST)			200K		

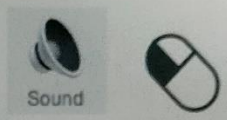
APPENDIX D: USB Omnidirectional Microphone Datasheet



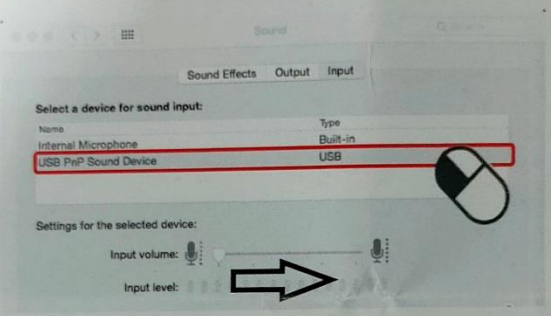
Installation-MAC BOOK:

1

2



3



Product Parameters

Technical Parameters	
Directivity	Omni directional
Frequency response	20Hz-20KHz
Sensitivity	-52dB
Signal to noise ratio	78dB
USB interface	USB 2.0
Power supply mode	USB DC5V
Material	Metal
Compatible	Windows XP/Vista/7/8/10/Mac

APPENDIX E: MPU9250 9-axis IMU Sensor Datasheet

3 Electrical Characteristics

3.1 Gyroscope Specifications

Typical Operating Circuit of section 4.2, VDD = 2.5V, VDDIO = 2.5V, T_A=25°C, unless otherwise noted.

PARAMETER	CONDITIONS	MIN	TYP	MAX	UNITS
Full-Scale Range	FS_SEL=0		±250		°/s
	FS_SEL=1		±500		°/s
	FS_SEL=2		±1000		°/s
	FS_SEL=3		±2000		°/s
Gyroscope ADC Word Length			16		bits
Sensitivity Scale Factor	FS_SEL=0		131		LSB/(°/s)
	FS_SEL=1		65.5		LSB/(°/s)
	FS_SEL=2		32.8		LSB/(°/s)
	FS_SEL=3		16.4		LSB/(°/s)
Sensitivity Scale Factor Tolerance	25°C		±3		%
Sensitivity Scale Factor Variation Over Temperature	-40°C to +85°C		±4		%
Nonlinearity	Best fit straight line; 25°C		±0.1		%
Cross-Axis Sensitivity			±2		%
Initial ZRO Tolerance	25°C		±5		°/s
ZRO Variation Over Temperature	-40°C to +85°C		±30		°/s
Total RMS Noise	DLPFCFG=2 (92 Hz)		0.1		°/s-rms
Rate Noise Spectral Density			0.01		°/s/√Hz
Gyroscope Mechanical Frequencies		25	27	29	KHz
Low Pass Filter Response	Programmable Range	5		250	Hz
Gyroscope Startup Time	From Sleep mode		35		ms
Output Data Rate	Programmable, Normal mode	4		8000	Hz

Table 1 Gyroscope Specifications

3.2 Accelerometer Specifications

Typical Operating Circuit of section 4.2, VDD = 2.5V, VDDIO = 2.5V, T_A=25°C, unless otherwise noted.

PARAMETER	CONDITIONS	MIN	TYP	MAX	UNITS
Full-Scale Range	AFS_SEL=0		±2		*g*
	AFS_SEL=1		±4		*g*
	AFS_SEL=2		±8		*g*
	AFS_SEL=3		±16		*g*
ADC Word Length	Output in two's complement format		16		bits
Sensitivity Scale Factor	AFS_SEL=0		16,384		LSB/*g*
	AFS_SEL=1		8,192		LSB/*g*
	AFS_SEL=2		4,096		LSB/*g*
	AFS_SEL=3		2,048		LSB/*g*
Initial Tolerance	Component-Level		±3		%
Sensitivity Change vs. Temperature	-40°C to +85°C AFS_SEL=0 Component-level		±0.026		%/°C
Nonlinearity	Best Fit Straight Line		±0.5		%
Cross-Axis Sensitivity			±2		%
Zero-G Initial Calibration Tolerance	Component-level, X,Y		±60		*mg*
	Component-level, Z		±80		*mg*
Zero-G Level Change vs. Temperature	-40°C to +85°C		±1.5		mg/°C
Noise Power Spectral Density	Low noise mode		300		µg/√Hz
Total RMS Noise	DLPFCFG=2 (94Hz)			8	mg-rms
Low Pass Filter Response	Programmable Range	5		260	Hz
Intelligence Function Increment			4		mg/LSB
Accelerometer Startup Time	From Sleep mode		20		ms
	From Cold Start, 1ms V_{DD} ramp		30		ms
Output Data Rate	Low power (duty-cycled)	0.24		500	Hz
	Duty-cycled, over temp		±15		%
	Low noise (active)	4		4000	Hz

Table 2 Accelerometer Specifications

3.3 Magnetometer Specifications

Typical Operating Circuit of section 4.2, VDD = 2.5V, VDDIO = 2.5V, T_A=25°C, unless otherwise noted.

PARAMETER	CONDITIONS	MIN	TYP	MAX	UNITS
MAGNETOMETER SENSITIVITY					
Full-Scale Range			±4800		µT
ADC Word Length			14		bits
Sensitivity Scale Factor			0.6		µT / LSB
ZERO-FIELD OUTPUT					
Initial Calibration Tolerance			±500		LSB

3.4 Electrical Specifications

3.4.1 D.C. Electrical Characteristics

Typical Operating Circuit of section 4.2, VDD = 2.5V, VDDIO = 2.5V, T_A=25°C, unless otherwise noted.

PARAMETER	CONDITIONS	MIN	TYP	MAX	Units	Notes
SUPPLY VOLTAGES						
VDD		2.4	2.5	3.6	V	
VDDIO		1.71	1.8	VDD	V	
SUPPLY CURRENTS						
Normal Mode	9-axis (no DMP), 1 kHz gyro ODR, 4 kHz accel ODR, 8 Hz mag. repetition rate		3.7		mA	
	6-axis (accel + gyro, no DMP), 1 kHz gyro ODR, 4 kHz accel ODR		3.4		mA	
	3-axis Gyroscope only (no DMP), 1 kHz ODR		3.2		mA	
	6-axis (accel + magnetometer, no DMP), 4 kHz accel ODR, mag. repetition rate = 8 Hz		730		µA	
	3-Axis Accelerometer, 4kHz ODR (no DMP)		450		µA	
	3-axis Magnetometer only (no DMP), 8 Hz repetition rate		280		µA	
Accelerometer Low Power Mode (DMP, Gyroscope, Magnetometer disabled)	0.98 Hz update rate		8.4		µA	1
	31.25 Hz update rate		19.8		µA	1
Full Chip Idle Mode Supply Current			8		µA	
TEMPERATURE RANGE						
Specified Temperature Range	Performance parameters are not applicable beyond Specified Temperature Range	-40		+85	°C	

Table 3 D.C. Electrical Characteristics

Notes:

1. Accelerometer Low Power Mode supports the following output data rates (ODRs): 0.24, 0.49, 0.98, 1.95, 3.91, 7.81, 15.63, 31.25, 62.50, 125, 250, 500Hz. Supply current for any update rate can be calculated as:

   Supply Current in µA = Sleep Current + Update Rate * 0.376

3.4.2 A.C. Electrical Characteristics

Typical Operating Circuit of section 4.2, VDD = 2.5V, VDDIO = 2.5V, T_A=25°C, unless otherwise noted.

Parameter	Conditions	MIN	TYP	MAX	Units
Supply Ramp Time	Monotonic ramp. Ramp rate is 10% to 90% of the final value	0.1		100	ms
Operating Range	Ambient	-40		85	°C
Sensitivity	Untrimmed		333.87		LSB/°C
Room Temp Offset	21°C		0		LSB
Supply Ramp Time (T_{RAMP})	Valid power-on RESET	0.01	20	100	ms
Start-up time for register read/write	From power-up		11	100	ms
I²C ADDRESS	AD0 = 0 AD0 = 1		1101000 1101001		
V_{IH}, High Level Input Voltage		0.7*VDDIO			V
V_{IL}, Low Level Input Voltage				0.3*VDDIO	V
C_I, Input Capacitance			< 10		pF
V_{OH}, High Level Output Voltage	R_{LOAD}=1MΩ;	0.9*VDDIO			V
V_{OL1}, LOW-Level Output Voltage	R_{LOAD}=1MΩ;			0.1*VDDIO	V
$V_{OL\,INT1}$, INT Low-Level Output Voltage	OPEN=1, 0.3mA sink Current			0.1	V
Output Leakage Current	OPEN=1		100		nA
t_{INT}, INT Pulse Width	LATCH_INT_EN=0		50		µs
V_{IL}, LOW Level Input Voltage		-0.5V		0.3*VDDIO	V
V_{IH}, HIGH-Level Input Voltage		0.7*VDDIO		VDDIO + 0.5V	V
V_{hys}, Hysteresis			0.1*VDDIO		V
V_{OL}, LOW-Level Output Voltage	3mA sink current	0		0.4	V
I_{OL}, LOW-Level Output Current	V_{OL}=0.4V V_{OL}=0.6V		3 6		mA mA
Output Leakage Current			100		nA
t_{of}, Output Fall Time from V_{IHmax} to V_{ILmax}	C_b bus capacitance in pf	20+0.1C_b		250	ns
V_{IL}, LOW-Level Input Voltage		-0.5V		0.3*VDDIO	V
V_{IH}, HIGH-Level Input Voltage		0.7* VDDIO		VDDIO + 0.5V	V
V_{hys}, Hysteresis			0.1* VDDIO		V
V_{OL1}, LOW-Level Output Voltage	VDDIO > 2V; 1mA sink current	0		0.4	V
V_{OL3}, LOW-Level Output Voltage	VDDIO < 2V; 1mA sink current	0		0.2* VDDIO	V
I_{OL}, LOW-Level Output Current	V_{OL} = 0.4V V_{OL} = 0.6V		3 6		mA mA
Output Leakage Current			100		nA
t_{of}, Output Fall Time from V_{IHmax} to V_{ILmax}	C_b bus capacitance in pF	20+0.1C_b		250	ns
Sample Rate	Fchoice=0,1,2 SMPLRT_DIV=0		32		kHz
	Fchoice=3; DLPFCFG=0 or 7 SMPLRT_DIV=0		8		kHz
	Fchoice=3; DLPFCFG=1,2,3,4,5,6; SMPLRT_DIV=0		1		kHz
Clock Frequency Initial Tolerance	CLK_SEL=0, 6; 25°C	-2		+2	%

	CLK_SEL=1,2,3,4,5; 25°C	-1		+1	%
Frequency Variation over Temperature	CLK_SEL=0,6	-10		+10	%
	CLK_SEL=1,2,3,4,5		±1		%

Table 4 A.C. Electrical Characteristics

3.4.3 Other Electrical Specifications

Typical Operating Circuit of section 4.2, VDD = 2.5V, VDDIO = 2.5V, T_A=25°C, unless otherwise noted.

PARAMETER	CONDITIONS	MIN	TYP	MAX	Units
SPI Operating Frequency, All Registers Read/Write	Low Speed Characterization		100 ±10%		kHz
	High Speed Characterization		1 ±10%		MHz
SPI Operating Frequency, Sensor and Interrupt Registers Read Only			20 ±10%		MHz
I^2C Operating Frequency	All registers, Fast-mode			400	kHz
	All registers, Standard-mode			100	kHz

Table 5 Other Electrical Specifications

3.5 I2C Timing Characterization

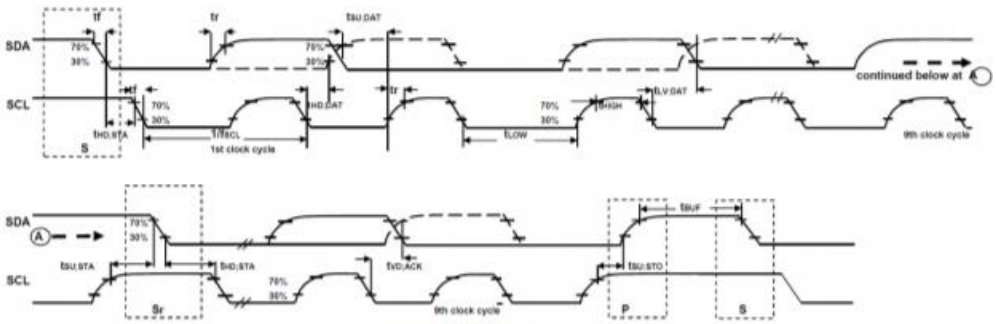
Typical Operating Circuit of section 4.2, VDD = 2.4V to 3.6V, VDDIO = 1.71 to VDD, T_A=25°C, unless otherwise noted.

Parameters	Conditions	Min	Typical	Max	Units	Notes
I²C TIMING	**I²C FAST-MODE**					
f_{SCL}, SCL Clock Frequency				400	kHz	
$t_{HD.STA}$, (Repeated) START Condition Hold Time		0.6			µs	
t_{LOW}, SCL Low Period		1.3			µs	
t_{HIGH}, SCL High Period		0.6			µs	
$t_{SU.STA}$, Repeated START Condition Setup Time		0.6			µs	
$t_{HD.DAT}$, SDA Data Hold Time		0			µs	
$t_{SU.DAT}$, SDA Data Setup Time		100			ns	
t_r, SDA and SCL Rise Time	C_b bus cap. from 10 to 400pF	20+0.1C_b		300	ns	
t_f, SDA and SCL Fall Time	C_b bus cap. from 10 to 400pF	20+0.1C_b		300	ns	
$t_{SU.STO}$, STOP Condition Setup Time		0.6			µs	
t_{BUF}, Bus Free Time Between STOP and START Condition		1.3			µs	
C_b, Capacitive Load for each Bus Line			< 400		pF	
$t_{VD.DAT}$, Data Valid Time				0.9	µs	
$t_{VD.ACK}$, Data Valid Acknowledge Time				0.9	µs	

Table 6 I²C Timing Characteristics

Notes:

- Timing Characteristics apply to both Primary and Auxiliary I2C Bus
- Based on characterization of 5 parts over temperature and voltage as mounted on evaluation board or in sockets



I²C Bus Timing Diagram

3.6 SPI Timing Characterization

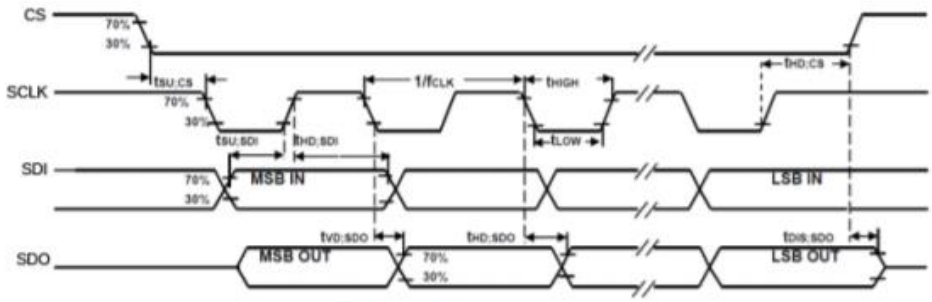
Typical Operating Circuit of section 4.2, VDD = 2.4V to 3.6V, VDDIO = 1.71V to VDD, T_A=25°C, unless otherwise noted.

Parameters	Conditions	Min	Typical	Max	Units	Notes
SPI TIMING						
f_{SCLK}, SCLK Clock Frequency				1	MHz	
t_{LOW}, SCLK Low Period		400			ns	
t_{HIGH}, SCLK High Period		400			ns	
$t_{SU:CS}$, CS Setup Time		8			ns	
$t_{HD:CS}$, CS Hold Time		500			ns	
$t_{SU:SDI}$, SDI Setup Time		11			ns	
$t_{HD:SDI}$, SDI Hold Time		7			ns	
$t_{VD:SDO}$, SDO Valid Time	C_{load} = 20pF			100	ns	
$t_{HD:SDO}$, SDO Hold Time	C_{load} = 20pF	4			ns	
$t_{DIS:SDO}$, SDO Output Disable Time				50	ns	

Table 7 SPI Timing Characteristics

Notes:

1. Based on characterization of 5 parts over temperature and voltage as mounted on evaluation board or in sockets



SPI Bus Timing Diagram

3.6.1 fSCLK = 20MHz

Parameters	Conditions	Min	Typical	Max	Units
SPI TIMING					
f_{SCLK}, SCLK Clock Frequency		0.9		20	MHz
t_{LOW}, SCLK Low Period		-		-	ns
t_{HIGH}, SCLK High Period		-		-	ns
$t_{SU:CS}$, CS Setup Time		1			ns
$t_{HD:CS}$, CS Hold Time		1			ns

$t_{SU,SDI}$, SDI Setup Time		0			ns
$t_{HD,SDI}$, SDI Hold Time		1			ns
$t_{VD,SDO}$, SDO Valid Time	C_{load} = 20pF		25		ns
$t_{DIS,SDO}$, SDO Output Disable Time				25	ns

Table 8 fCLK = 20MHz

Note:

1. Based on characterization of 5 parts over temperature and voltage as mounted on evaluation board or in sockets

3.7 Absolute Maximum Ratings

Stress above those listed as "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only and functional operation of the device at these conditions is not implied. Exposure to the absolute maximum ratings conditions for extended periods may affect device reliability.

Specification	Symbol	Conditions	MIN	MAX	Units
Supply Voltage	V_{DD}		-0.5	4.0	V
	V_{DDIO}		-0.5	4.0	V
Acceleration		Any axis, unpowered, 0.2ms duration		10,000	*g*
Temperature		Operating	-40	105	°C
		Storage	-40	125	°C
ESD Tolerance		HBM	2		KV
		MM	250		V

APPENDIX F: Buzzer Datasheet

Buzzer

pro-SIGNAL

RoHS Compliant

Features

- Black in colour
- With internal drive circuit
- Sealed structure
- Wave solderable and washable
- Housing material: Noryl

Applications

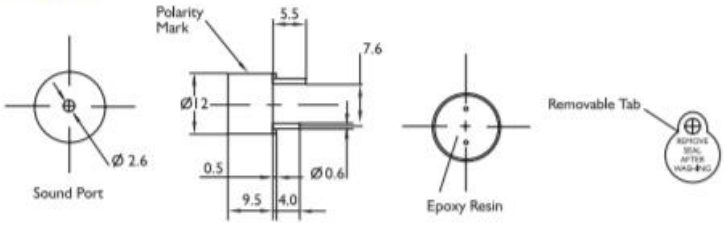
- Computer and peripherals
- Communications equipment
- Portable equipment
- Automobile electronics
- POS system
- Electronic cash register

Specifications:

Rated Voltage	: 6V DC
Operating Voltage	: 4 to 8V DC
Rated Current*	: ≤30mA
Sound Output at 10cm*	: ≥85dB
Resonant Frequency	: 2300 ±300Hz
Tone	: Continuous
Operating Temperature	: -25°C to +80°C
Storage Temperature	: -30°C to +85°C
Weight	: 2g

*Value applying at rated voltage (DC)

Diagram



Dimensions : Millimetres
Tolerance : ±0.5mm

Part Number Table

Description	Part Number
Buzzer, Electromech, 6V DC	ABI-009-RC

APPENDIX G: GY-NEO6MV2 GPS Tracking Module Datasheet

1.3 GPS performance

Parameter	Specification			
Receiver type	50 Channels GPS L1 frequency, C/A Code SBAS: WAAS, EGNOS, MSAS			
Time-To-First-Fix[1]		NEO-6G/Q/T	NEO-6M/V	NEO-6P
	Cold Start[2]	26 s	27 s	32 s
	Warm Start[2]	26 s	27 s	32 s
	Hot Start[2]	1 s	1 s	1 s
	Aided Starts[3]	1 s	<3 s	<3 s
Sensitivity[4]		NEO-6G/Q/T	NEO-6M/V	NEO-6P
	Tracking & Navigation	-162 dBm	-161 dBm	-160 dBm
	Reacquisition[5]	-160 dBm	-160 dBm	-160 dBm
	Cold Start (without aiding)	-148 dBm	-147 dBm	-146 dBm
	Hot Start	-157 dBm	-156 dBm	-155 dBm
Maximum Navigation update rate		NEO-6G/Q/M/T	NEO-6P/V	
		5Hz	1 Hz	
Horizontal position accuracy[6]	GPS	2.5 m		
	SBAS	2.0 m		
	SBAS + PPP[7]	< 1 m (2D, R50)[8]		
	SBAS + PPP[7]	< 2 m (3D, R50)[8]		
Configurable Timepulse frequency range		NEO-6G/Q/M/P/V	NEO-6T	
		0.25 Hz to 1 kHz	0.25 Hz to 10 MHz	
Accuracy for Timepulse signal	RMS	30 ns		
	99%	<60 ns		
	Granularity	21 ns		
	Compensated[9]	15 ns		
Velocity accuracy[6]		0.1m/s		
Heading accuracy[6]		0.5 degrees		
Operational Limits	Dynamics	≤ 4 g		
	Altitude[10]	50,000 m		
	Velocity[10]	500 m/s		

Table 2: NEO-6 GPS performance

[1] All satellites at -130 dBm
[2] Without aiding
[3] Dependent on aiding data connection speed and latency
[4] Demonstrated with a good active antenna
[5] For an outage duration ≤10s
[6] CEP, 50%, 24 hours static, -130dBm, SEP: <3.5m
[7] NEO-6P only
[8] Demonstrated under following conditions: 24 hours, stationary, first 600 seconds of data discarded. HDOP < 1.5 during measurement period, strong signals. Continuous availability of valid SBAS correction data during full test period.
[9] Quantization error information can be used with NEO-6T to compensate the granularity related error of the timepulse signal
[10] Assuming Airborne <4g platform

3 Electrical specifications

3.1 Absolute maximum ratings

Parameter	Symbol	Module	Min	Max	Units	Condition
Power supply voltage	VCC	NEO-6G	-0.5	2.0	V	
		NEO-6Q, 6M, 6P, 6V, 6T	-0.5	3.6	V	
Backup battery voltage	V_BCKP	All	-0.5	3.6	V	
USB supply voltage	VDDUSB	All	-0.5	3.6	V	
Input pin voltage	Vin	All	-0.5	3.6	V	
	Vin_usb	All	-0.5	VDDUSB	V	
DC current trough any digital I/O pin (except supplies)	Ipin			10	mA	
VCC_RF output current	ICC_RF	All		100	mA	
Input power at RF_IN	Prfin	NEO-6Q, 6M, 6G, 6V, 6T		15	dBm	source impedance = 50Ω, continuous wave
		NEO-6P		-5	dBm	
Storage temperature	Tstg	All	-40	85	°C	

Table 9: Absolute maximum ratings

GPS receivers are Electrostatic Sensitive Devices (ESD) and require special precautions when handling. For more information see chapter 6.4.

Stressing the device beyond the "Absolute Maximum Ratings" may cause permanent damage. These are stress ratings only. The product is not protected against overvoltage or reversed voltages. If necessary, voltage spikes exceeding the power supply voltage specification, given in table above, must be limited to values within the specified boundaries by using appropriate protection diodes. For more information see the *LEA-6/NEO-6/MAX-6 Hardware Integration Manual* [1].

3.2 Operating conditions

All specifications are at an ambient temperature of 25°C.

Parameter	Symbol	Module	Min	Typ	Max	Units	Condition
Power supply voltage	VCC	NEO-6G	1.75	1.8	1.95	V	
		NEO-6Q/M NEO-6P/V/T	2.7	3.0	3.6	V	
Supply voltage USB	VDDUSB	All	3.0	3.3	3.6	V	
Backup battery voltage	V_BCKP	All	1.4		3.6	V	
Backup battery current	I_BCKP	All		22		µA	V_BCKP = 1.8 V, VCC = 0V
Input pin voltage range	Vin	All	0		VCC	V	
Digital IO Pin Low level input voltage	Vil	All	0		0.2*VCC	V	
Digital IO Pin High level input voltage	Vih	All	0.7*VCC		VCC	V	
Digital IO Pin Low level output voltage	Vol	All			0.4	V	Iol=4mA
Digital IO Pin High level output voltage	Voh	All	VCC -0.4			V	Ioh=4mA
USB_DM, USB_DP	VinU	All	Compatible with USB with 22 Ohms series resistance				
VCC_RF voltage	VCC_RF	All		VCC-0.1		V	
VCC_RF output current	ICC_RF	All			50	mA	
Antenna gain	Gant	All			50	dB	
Receiver Chain Noise Figure	NFtot	All		3.0		dB	
Operating temperature	Topr	All	-40		85	°C	

Table 10: Operating conditions

Operation beyond the specified operating conditions can affect device reliability.

3.3 Indicative power requirements

Table 11 lists examples of the total system supply current for a possible application.

Parameter	Symbol	Module	Min	Typ	Max	Units	Condition
Max. supply current [15]	Iccp	All			67	mA	VCC = 3.6 V[16] / 1.95 V[17]
Average supply current[18]	Icc Acquisition	All		47[19]		mA	VCC = 3.0 V[16] / 1.8 V[17]
	Icc Tracking (Max Performance mode)	NEO-6G/Q/T		40[20]		mA	
		NEO-6M/P/V		39[20]		mA	
	Icc Tracking (Eco mode)	NEO-6G/Q/T		38[20]		mA	
		NEO-6M/P/V		37[20]		mA	
	Icc Tracking (Power Save mode / 1 Hz)	NEO-6G/Q		12[20]		mA	
		NEO-6M		11[20]		mA	

Table 11: Indicative power requirements

Values in Table 11 are provided for customer information only as an example of typical power requirements. Values are characterized on samples, actual power requirements can vary depending on FW version used, external circuitry, number of SVs tracked, signal strength, type of start as well as time, duration and conditions of test.

[15] Use this figure to dimension maximum current capability of power supply. Measurement of this parameter with 1 Hz bandwidth.
[16] NEO-6Q, NEO-6M, NEO-6P, NEO-6V, NEO-6T
[17] NEO-6G
[18] Use this figure to determine required battery capacity.
[19] >8 SVs in view, CNo >40 dBHz, current average of 30 sec after cold start.
[20] With strong signals, all orbits available. For Cold Starts typical 12 min after first fix. For Hot Starts typical 15 s after first fix.

3.4 SPI timing diagrams

In order to avoid a faulty usage of the SPI, the user needs to comply with certain timing conditions. The following signals need to be considered for timing constraints:

Symbol	Description
SS_N	Slave Select signal
SCK	Slave Clock signal

Table 12: Symbol description

Figure 3: SPI timing diagram

3.4.1 Timing recommendations

Parameter	Description	Recommendation
t_{INIT}	Initialization Time	500 µs
t_{DES}	Deselect Time	1 ms
Bitrate		100 kbit/s

Table 13: SPI timing recommendations

The values in the above table result from the requirement of an error-free transmission. By allowing just a few errors, the byte rate could be increased considerably. These timings – and therefore the byte rate – could also be improved by disabling other interfaces, e.g. the UART.

The maximum bandwidth is 100 kbit/s[21].

[21] This is a theoretical maximum, the protocol overhead is not considered.

APPENDIX H: SIM800L GSM Module Datasheet

1. Introduction

This document describes SIM800L hardware interface in great detail.
This document can help user to quickly understand SIM800L interface specifications, electrical and mechanical details. With the help of this document and other SIM800L application notes, user guide, users can use SIM800L to design various applications quickly.

2. SIM800L Overview

SIM800L is a quad-band GSM/GPRS module, that works on frequencies GSM850MHz, EGSM900MHz, DCS1800MHz and PCS1900MHz. SIM800L features GPRS multi-slot class 12/ class 10 (optional) and supports the GPRS coding schemes CS-1, CS-2, CS-3 and CS-4.

With a tiny configuration of 15.8*17.8*2.4mm, SIM800L can meet almost all the space requirements in user applications, such as smart phone, PDA and other mobile devices.

SIM800L has 88pin pads of LGA packaging, and provides all hardware interfaces between the module and customers' boards.

- Support 5*5*2 keypads
- One full modem serial port, user can configure two serial ports
- One USB, the USB interfaces can debug, download software
- Audio channel which includes two microphone input; a receiver output and a speaker output
- Programmable general purpose input and output
- A SIM card interface
- Support FM
- Support one PWM

SIM800L is designed with power saving technique so that the current consumption is as low as 0.7mA in sleep mode.

2.1. SIM800L Key Features

Table 1: SIM800L key features

Feature	Implementation
Power supply	3.4V ~4.4V
Power saving	typical power consumption in sleep mode is 0.7mA (AT+CFUN=0)
Frequency bands	• Quad-band: GSM 850, EGSM 900, DCS 1800, PCS 1900. SIM800L can search the 4 frequency bands automatically. The frequency bands can also be set by AT command "AT+CBAND". For details, please refer to document [1]. • Compliant to GSM Phase 2/2+
Transmitting power	• Class 4 (2W) at GSM 850 and EGSM 900 • Class 1 (1W) at DCS 1800 and PCS 1900
GPRS connectivity	• GPRS multi-slot class 12（default） • GPRS multi-slot class 1~12 (option)
Temperature range	• Normal operation: -40°C ~ +85°C

	● Storage temperature -45°C ~ +90°C
Data GPRS	● GPRS data downlink transfer: max. 85.6 kbps ● GPRS data uplink transfer: max. 85.6 kbps ● Coding scheme: CS-1, CS-2, CS-3 and CS-4 ● PAP protocol for PPP connect ● Integrate the TCP/IP protocol. ● Support Packet Broadcast Control Channel (PBCCH) ● CSD transmission rates：2.4，4.8，9.6，14.4 kbps
CSD	● Support CSD transmission
USSD	● Unstructured Supplementary Services Data (USSD) support
SMS	● MT, MO, CB, Text and PDU mode ● SMS storage: SIM card
SIM interface	Support SIM card: 1.8V, 3V
External antenna	Antenna pad
Audio features	Speech codec modes: ● Half Rate (ETS 06.20) ● Full Rate (ETS 06.10) ● Enhanced Full Rate (ETS 06.50 / 06.60 / 06.80) ● Adaptive multi rate (AMR) ● Echo Cancellation ● Noise Suppression
Serial port and debug port	**Serial port:** ● Full modem interface with status and control lines, unbalanced, asynchronous. ● 1200bps to 115200bps. ● Can be used for AT commands or data stream. ● Support RTS/CTS hardware handshake and software ON/OFF flow control. ● Multiplex ability according to GSM 07.10 Multiplexer Protocol. ● Autobauding supports baud rate from 1200 bps to 57600bps. ● upgrading firmware **Debug port:** ● USB_DM and USB_DP ● Can be used for debugging and upgrading firmware.
Phonebook management	Support phonebook types: SM, FD, LD, RC, ON, MC.
SIM application toolkit	GSM 11.14 Release 99
Real time clock	Support RTC
Timing functions	Use AT command set
Physical characteristics	Size:15.8*17.8*2.4mm Weight:1.35g
Firmware upgrade	Main serial port or USB port.

Table 2: Coding schemes and maximum net data rates over air interface

Coding scheme	1 timeslot	2 timeslot	4 timeslot
CS-1	9.05kbps	18.1kbps	36.2kbps
CS-2	13.4kbps	26.8kbps	53.6kbps
CS-3	15.6kbps	31.2kbps	62.4kbps
CS-4	21.4kbps	42.8kbps	85.6kbps

2.2. Operating Mode

The table below summarizes the various operating modes of SIM800L.

Table 3: Overview of operating modes

Mode	Function	
Normal operation	GSM/GPRS SLEEP	Module will automatically go into sleep mode if the conditions of sleep mode are enabling and there is no on air and no hardware interrupt (such as GPIO interrupt or data on serial port). In this case, the current consumption of module will reduce to the minimal level. In sleep mode, the module can still receive paging message and SMS.
	GSM IDLE	Software is active. Module is registered to the GSM network, and the module is ready to communicate.
	GSM TALK	Connection between two subscribers is in progress. In this case, the power consumption depends on network settings such as DTX off/on, FR/EFR/HR, hopping sequences, antenna.
	GPRS STANDBY	Module is ready for GPRS data transfer, but no data is currently sent or received. In this case, power consumption depends on network settings and GPRS configuration.
	GPRS DATA	There is GPRS data transfer (PPP or TCP or UDP) in progress. In this case, power consumption is related with network settings (e.g. power control level); uplink/downlink data rates and GPRS configuration (e.g. used multi-slot settings).
Power down	Normal power down by sending AT command "AT+CPOWD=1" or using the PWRKEY. The power management unit shuts down the power supply for the baseband part of the module, and only the power supply for the RTC is remained. Software is not active. The serial port is not accessible. Power supply (connected to VBAT) remains applied.	
Minimum functionality mode	AT command "AT+CFUN" can be used to set the module to a minimum functionality mode without removing the power supply. In this mode, the RF part of the module will not work or the SIM card will not be accessible, or both RF part and SIM card will be closed, and the serial port is still accessible. The power consumption in this mode is lower than normal mode.	

APPENDIX I: CH340G USB to TTL Converter Module Datasheet

ANDROEGG Data sheet: CH340G USB to UART Interface

CH340G USB to UART Interface

Data sheet: CH340G USB to UART Interface

Technical Informations:

CH340 is a series of USB bus adapters, that provides serial, parallel or IrDA interfaces over USB bus (only serial interface). The CH340G integrate circuit provides common MODEM signals to allow adding a UART Devices to a computer, or converting existing UART devices to USB interface.

Features:

- ✓ provides a virtual serial port over USB 2.0 port
- ✓ full speed 2.0 USB interface
- ✓ based on 340G chip
- ✓ supports operating systems as follows:
  - Linux
  - Mac OSX
  - Windows
- ✓ supports baud rates from 50 bps up to 2 Mbps
- ✓ supports CH341 driver
- ✓ rail voltage
  - 5V mode 4.5-5.5V
  - 3.3V mode 3.3-3.8V
- ✓ Operating current typ. 12 mA up to 30mA [1]
- ✓ Clock-frequency typ. 12 MHz.
- ✓ Power-on reset time typ. 20 ms up to 50 ms
- ✓ USB A Connector (male)
- ✓ Transmitter baud rate error less than 0,3%
- ✓ Receiver baud rate tolerance < 2%

[1] *please see Important Notes*

Dimensions:

Dimension	incl. Pins	w/o Pins
length	52 mm	45 mm
width	14 mm	14 mm
height	8,5 mm	8,5 mm
weight	5 gr.	5 gr.

Important Notes:

CH340G maximum operating current is 30 mA, **running ESP8266 directly from CH340G is not recommended.**

Typical ESP8266EX current consumption range (w/o SPI Flash):

- deep sleep 10 µA
- Modem sleep 15 mA
- Modem active 50 - 170 mA

CH340G Driver Installation

Actual Driver download overview:

Operating System	download Link
Linux	CH341SER_LINUX_OS.zip
MAC OSX	CH341SER_MAC_OS.zip
Windows	CH341SER_WINDOWS_OS.zip
Android	CH341SER_ANDROID_OS.zip

1. please choose designated download link
2. unpack zip file
3. run installer package

CH341 common Driver Problems

Mac OSX 10.9 Mavericks Mac OSX 10.10 Yosemite

On newer versions of OS X (10.9 and 10.10), when you double-click the install packages inside the CH341 disk image, you may be presented with a type error about not being able to open the files because they are not from an identified developers.

temporarily Solution

4. To get around this, simply **right-click at the CH341 installer package** you want to install, or press **CTRL + mouse click**, if you don't have a right-click. Then **select open** from the menu.
5. A new dialog will open asking if you are certain
   - .. Are you sure you want to open it?
   - **Click Open**, and proceed with the installation

permanent Solution

OSX default setting allows only installing Applications downloaded from App Store or identified developers. **Caution**, this solution will allow installing applications downloaded from any resources!

1. Open **System Preference**
2. If System Preferences appear **click on Security & Privacy** Settings
   - **click on lock sign** for enable making changes
   - assign Administrator privileges within password
   - choose **Anywhere**
3. A new dialog will open
   - Choosing "Anywhere" makes your Mac less secure
   - Click Allow From Anywhere
4. Double Click on CH341 Installer package and proceed with installation of CH341

Mac OSX 10.11 El Capitan

Depending on version of OSX 10.11 EL Capitan will allow (or not) temporarily solution, also on some systems installation of Kext File will be interrupted. Either way temporarily Solution as follows is recommended.

temporarily Solution

1. For installing CH341 driver, simply **right-click at the CH341 installer package** you want to install, if you don't have enabled right-click in System Preferences, Mouse settings **CTRL + mouse click**. Then **select open** from the menu.
2. A new dialog will open asking if you are certain
   - ... Are you sure you want to open it?
   - **Click Open**, and proceed with the installation

If installation fails, OSX EL Capitan will not allow installing required Kext Files, proceed installation with permanent Solution.

permanent Solution

OSX EL Capitan will not allow change system preference / security settings during running OSX. OSX El Capitan must restarted in recovery mode, **please read steps as follows carefully**.

1. **Close all Applications, save all Files**
2. In the Apple menu , choose **Restart**
3. As the computer restarts, hold down the **Command (⌘)** in **combination** with **R key**.
   Apple sign will appear for a while (up to couple of minutes) until recovery mode will appear.
4. In recovery mode click on **System Preference**
5. In System Preference **click on Security & Privacy** Settings,
   - **click on lock sign** for enable making changes
   - assign Administrator privileges within **password**
   - choose **Anywhere**
6. A new dialog will open
   - Choosing "Anywhere" makes your Mac less secure
   - Click **Allow From Anywhere**
7. After saving Security & Privacy Settings restart by click on choose **Restart**
8. After restart **double click on designated CH341 Installer package** and proceed with installation of CH341
   - For restore EL Capitan security setting please follow step 9 to 13

Restore El Capitan security settings

For security reasons it is recommended change security settings to OSX El Capitan default settings.

9. After installing CH341 Package click Apple menu , choose **Restart**
10. As the computer restarts, hold down the **Command (⌘)** in **combination** with **R key**. Apple sign will appear for a while (up to couple of minutes) until recovery mode will appear.
11. In recovery mode click on **System Preference**
12. In System Preference **click on Security & Privacy** Settings.
    - **click on lock sign** for enable making changes
    - assign Administrator privileges within **password**
    - choose Mac App Store and identified developers
13. After saving Security & Privacy Settings restart by click on choose **Restart**

After restart CH341 driver will be installed and security settings will be default El Capitan settings.

In case of error messages during driver install kext privileges has to be changed (see next chapter Changing OSX El Capitan kext privileges).

Changing OSX El Capitan kext privileges

Normally, whole directory that contains the kext files must be owned by the **root:wheel** user. If it's not, errors during loading phase of kext (kernel extension) will appear. Depending on OSX El Capitan version System Integrity Protection has to be disabled in recovery mode as follows.

1. **Close all Applications, save all Files**
2. In the Apple menu , choose **Restart**
3. As the computer restarts, hold down the **Command (⌘)** in **combination** with **R key**. Apple sign will appear for a while (up to couple of minutes) until recovery mode will appear.
4. In recovery mode click on **Utilities menu choose Security Configuration**
5. In System Configuration **disable System Integrity Protection** checkbox
    - **click on apply** for enable making changes
6. after rebooting, restart Mac kext files will be writable, if not please follow next solution.

Depending on OSX 10.11 version previous version will not work, because of NVRAM options. On some system you can change kext privileges by using Terminal in regular mode, so if following steps are not working change system into recovery mode as in previous solution.

1. Open Terminal
    - in regular mode **Launchpad** find **others click Terminal**
    - in recovery mode **Utilities menu choose Terminal**
2. In Terminal check System Integrity Protection status by using command as follows
    - **sudo csrutil status** press ↩ (enter)
    - assign Administrator privileges within **password** (password will not appear) and **press** ↩ (enter)
    - message as follows will appear **System Integrity Protection status: enabled.**

3. For changing System Integrity Protection status use command as follows
   - csrutil disable **press** ↩ (enter)
   - message as follows will appear **Successfully disabled System Integrity Protection. Please restart the machine for changes to take effect.**
   - Follow instructions as above

Linux

CH341 Driver is already preconfigured in Linux Kernel.

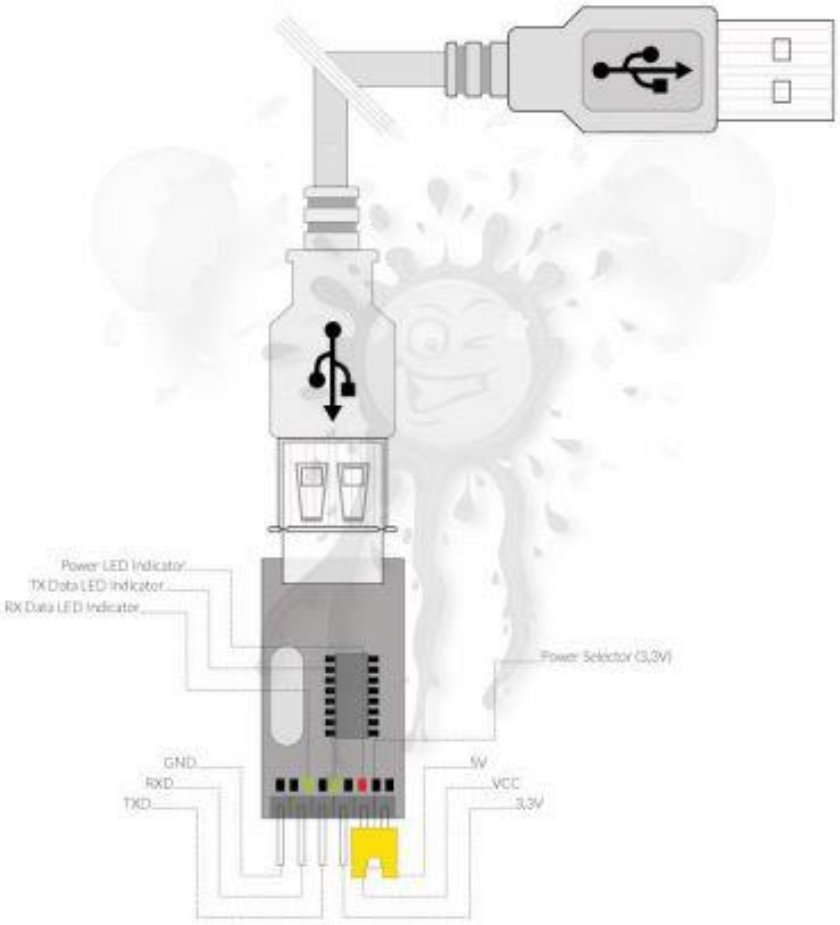
Windows

Until now no issues during CH341 Windows Installation are known. If problems during installation appear don't hesitate contacting us by mail.

Android

CH341SER_ANDROID_OS Driver Package is based on typical Android OS. For running CH340G on Android x86 within virtual machine (VirtualBox,...) Driver Package has to be installed on host system. Within our experience until now USB is not supported on X86 Virtual Machines.

Drawing CH340 USB TTL Converter



CH340G Pinout