DESIGN AND DEVELOPMENT OF A PORTABLE SECURITY SYSTEM FOR A BICYCLE

By

ANIRBAN MAITY

B.TECH (MECHANICAL ENGINEERING), 2015

MAKAUT (f. k. a WBUT)

EXAMINATION ROLL NUMBER: **M4PRD19016**

REGISTRATION NUMBER: **140928 of 2017-18**

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF **MASTER OF PRODUCTION ENGINEERING** IN THE FACULTY OF ENGINEERING AND TECHNOLOGY

JADAVPUR UNIVERSITY, 2019

DEPARTMENT OF PRODUCTION ENGINEERING

JADAVPUR UNIVERSITY

KOLKATA-700032

INDIA

JADAVPUR UNIVERSITY

FACULTY OF ENGINEERING AND TECHNOLOGY

CERTIFICATE OF RECOMMEDATION

I HEREBY RECOMMEND THAT THE THESIS ENTITLED "**DESIGN AND DEVELOPMENT OF A PORTABLE SECURITY SYSTEM FOR A BYCYCLE**" CARRIED OUT UNDER MY GUIDANCE BY **MR. ANIRBAN MAITY** MAY BE ACCEPTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF "**MASTER OF PRODUCTION ENGINEERING**".

- -

Prof. (Dr.) Soumya Sarkar
Thesis Advisor
Dept. of Production Engineering
Jadavpur University
Kolkata-700032

- -

HEAD, Dept. of Production Engineering
Jadavpur University
Kolkata-700032

- -

DEAN, Faculty of Engineering and Technology
Jadavpur University
Kolkata-700032

JADAVPUR UNIVERSITY

FACULTY OF ENGINEERING AND TECHNOLOGY

CERTIFICATE OF APPROVAL*

The foregoing thesis is hereby approved as a creditable study of an engineering subject carried out and presented in a manner of satisfactory to warrant its acceptance as a pre-requisite to the degree for which it has been submitted. It is understood that by this approval, the undersigned do not necessarily endorse or approve any statement made, opinion expressed and conclusion drawn therein but thesis only for the purpose for which it has been submitted.

COMMITTEE ON
FINAL EXAMINATION
FOR EVALUATION OF
THE THESIS

- -

- -

- -

*only in case the recommendation is concurred in

DECLARATION OF ORIGINALITY AND COMPLIANCE OF ACADEMIC ETHICS

I hereby declare that this thesis contains literature survey and original research work by the undersigned, as a part of Master of Production Engineering studies. All information in this document have been obtained and presented in accordance with the academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

_____

NAME: ANIRBAN MAITY

EXAMINATION ROLL NUMBER: M4PRD19016

REGISTRATION NUMBER: 140928 OF 2017-2018

Thesis title: "DESIGN AND DEVELOPMENT OF A PORTABLE SECURITY SYTEM FOR A BICYCLE."

ACKNOWLEDGEMENT

I owe a deepest debt of gratitude to my respected teacher, mentor and project supervisor, Prof. (Dr.) Soumya Sarkar, Dept. Of Production Engineering, Jadavpur University for his invaluable and untiring guidance, encouragement and supervision, throughout this thesis work. His effective skill, knowledge and experience have made it possible for me to successfully complete this thesis work within stipulated time. I am very much indebted to him and express my sincere gratitude to him.

I also take this opportunity to express my gratitude to all the faculty members of Production Engineering department for their mental support, immense help and co-operation during the course of this thesis work.

I would like to express my deep respect to Mr. Manas Kumar Pathak, Scientific Officer - G & OIC, AERB, for his guidance in completion of the project. I would also like to express my gratitude to Mr. Barun Kumar Das, Former Asst. Manager (Eng.), BIECCO LAWRIE Ltd for his unparallel guidance towards implementing the circuit on Vero board. I am greatly thankful to them for their constant motivation.

I express my heartiest thanks to all my friends and Research scholars of production engineering department, Jadavpur University for their cordial assistance and support. I am also thankful to Narendranath Dutta, UG student for helping me in the programming language.

Finally, special thanks to my beloved parent and sister, as they have always stood by me, caring least the prevalent situation.

……

ANIRBAN MAITY

Table of Contents

Chapter 1

Introduction

Security system is means or method by which something is secured through a system of interworking components and devices. Typical security systems are networks of integrated electronic devices working together with a central control panel to protect against burglars and other potential intruders. Surveillance, from homes to industries, plays a significant role in the fulfilment of our security. Surveillance can be done by use of electronic equipment like CCTV cameras. However, CCTV technology is expensive for average residents to install. Additionally, this kind of system does not notify the user immediately a burglary occurs. Generally All security systems work on the same basic principle of securing particular points, like doors and windows, as well as interior space containing valuables like art, computers, guns, and coin collections, and also there are some security systems which focuses on portability of it. An anti-theft system is any device or method used to prevent or deter the unauthorized appropriation of items considered valuable. Theft is one of the most common and oldest criminal behaviours. From the invention of the first lock and key to the introduction of RFID tags and biometric identification, anti-theft systems have evolved to match the introduction of new inventions to society and the resulting theft by others. Regardless of the number of items an owner decides to protect, the only real difference is in the number of security components used and monitored by the control panel. Human's tends to use security systems for their homes or cars or bikes against intruder and unauthorized access to their valuable things. Security alarms in residential areas show a correlation with decreased theft. Car alarms likewise help protect vehicles and their contents. Prisons also use security systems for control of inmates. It is very often true that people's perception of security is not directly related to actual security. For example, a fear of flying is much more common than a fear of driving; however, driving is generally a much more dangerous form of transport . According to Marston, R. M., (1998) modern electronics security system range in complexity from simple electronic door-bell to ultra-sophisticated wireless burglar alarm system that comes complete with an array of passive infra-red (PIR) movement detectors and contact sensors plus full remote-control and sensor monitoring facilities. The idea of

electronics-based security system has a wide range of application. They can be designed to be activated by physical contact or body proximity, or by variation in heat, light, or infrared radiation levels, or in voltage, current, resistance or some other electrical properties and parameters (Marston, 1998).

1.1 Definition of Security:

Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security. The word "security" in general usage is synonymous with "safety," but as a technical term "security" means that something not only is secure but that it has been secured .In other words security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others. Beneficiaries (technically referents) of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change by its environment. Security mostly refers to protection from hostile forces, but it has a wide range of other senses: for example, as the absence of harm (e.g. freedom from want); as the presence of an essential good (e.g. food security); as resilience against potential damage or harm (e.g. secure foundations); as secrecy (e.g. a secure telephone line); as containment (e.g. a secure room or cell); and as a state of mind (e.g. emotional security). The term security is used in this thesis report to designate security of our valuable items in public places, valuable items may cover our backpack that we used as our companion in any travelling purposes or may be our 4 wheeler or may be our two wheeler that is needed to be protect from burgling and theft. A vehicle is usually the most expensive and important asset next to a home, so this system enables you to keep this asset secure form any burgling or theft threat.

1.2 Need for an antitheft alarm system:

Items may require an anti-theft alarm based security system for a variety of reasons, which may occur in combination depending on the type of item and its purpose:

- The item is expensive and/or has sentimental value (prestigious car, family heirloom, birthday gift, war medals, coin collection)
- The item is difficult/impossible to replace if lost (produced in low numbers, antiques, unique works of art)

- The item is easy to steal (retail/supermarket products, office stationery)
- The item may be left unattended in an unsafe environment for a certain amount of time (laptop in a library, car in a car park)
- Improper use of the item may cause considerable damage or encourage further unauthorized actions (theft of car keys, stolen building access keys, identity theft)
- The item is desirable to others (jewellery, mobile phones, rare collectibles, auto parts, industrial designs)
- The item is otherwise unobtainable: (Alcohol, Tobacco products, age related substances).

1.3 Alarm based security systems:

So far we have discussed about the concepts of security through our daily experiences. With an improved awareness of the importance of security, bi-cycle manufacturer/owners are on the lookout for an efficient surveillance system which is low cost and user friendly.

Now we will try to integrate the concepts of security towards an alarming device that will let us know or more precisely alert us of any theft or burgling of Bi-cycles.

For alarm based security systems to work there should be some sensor or sensors to detect any unwanted intrusion or any unwanted activity of a stranger, then that sensor will prompt microcontroller to work accordingly to let us know that there is an attempt to theft or burgling, so that we can take necessary steps. A basic block diagram designed for an alarm based security system presented below-

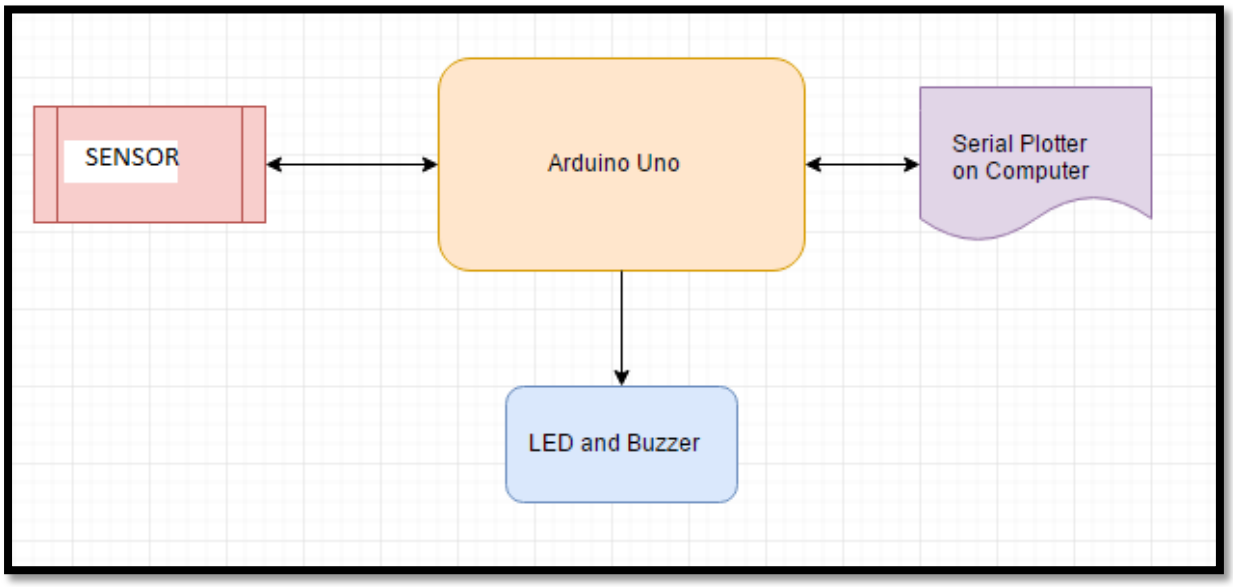


Fig 1.1: Block diagram of security system

So from the above block diagram it is very clear that for a security system to work the basic thing that we need is sensor and a detecting media that will eventually let us know that there is some intrusion or burgling or theft attempt is going on. So this types of security system scan be made where sensors communicate with a controller and gives alarm. This device can typically place in a place like below the seat of the bi-cycle so that the same cannot be easily identified by the burglar but the same can detect very easily if there is any sort of irregular activity is going on or not.

Following are the major common components of the security device-

a) **Control panel:** The control panel is the brain behind the security devices that arms and disarms the security systems, communicates with each installed component, sounds the alarm when there is an intrusion or any theft or burgling is going on,.In modern systems, this is typically one or more computer circuit boards inside a metal enclosure, along with a power supply. They typically feature a touchpad button panels for easy programming and interaction, is where pass codes are entered to arm and disarm the system, can work on voice commands, and can be programmed to work with wireless remote controls.

b) **Sensors:** This the most important part of any alarm based security systems as it will interact with the outside world or more precisely it will sense any unwanted attempts of burglary. When the security system is armed at the control panel, these sensors communicate with it by reporting that there is no attempt of burgling or theft. Should a monitored vehicle or bicycle suddenly be moved by some persons with motives of burgling, the security system is alerted and the control panel interprets this as a breach of a secured item. A high-decibel alarm is sounded. And the people in the surroundings are notified. These security components, when armed, protect a given degree of movement by creating an invisible zone that cannot be breached without sounding an alarm. These are typically used to protect backpacks containing valuables, vehicles be it two wheeler or three wheeler, as well as valuable items in our home.

c) **Alerting devices:** Alerting devices in a security system is used to alert the operator/owner/surroundings of any wrong doings. In other words this is the device that will let people know if there is any burglary attempt or not. Without this we can no act against any burglary attempt. These indicate an alarm condition. Most

commonly, these are bells, sirens, and/or flashing lights. Alerting devices serve the dual purposes of warning occupants of intrusion, and potentially scaring off burglars.

d) **Interconnections:** Interconnections means interconnectors between the components, this may consist of direct wiring to the control unit, or wireless links with local power supplies.

In addition to the system itself, security alarms are often coupled with a monitoring service. In the event of an alarm, the premises control unit contacts a central monitoring station. Operators at the station see the signal and take appropriate action, such as contacting property owners, notifying police, or dispatching private security forces. Such signals may be transmitted via dedicated alarm circuits, telephone lines, or the internet.

1.4 Factors Considered in designing an Anti-theft alarm system:

Equally varied are the methods developed for theft prevention. Anti-theft systems have evolved to counter new theft techniques as they have appeared in society. The choice for a particular anti-theft system is dependent on the following factors:

a) Financial cost:

In addition to the initial obtainable cost of an item, the cost of replacement or recovery from theft of the item is usually considered when considering the cost of installing an anti-theft system. This cost estimation usually determines the maximum cost of the anti-theft system and the need to secure it. Expensive items will generally be secured with a higher cost anti-theft system, while low-cost items will generally be secured at a lower cost. Insurance companies will often mandate a minimum type of anti-theft system as part of the conditions for insurance.

b) Threshold for theft:

Anti-theft systems are designed to raise the difficulty of theft to an infeasible (but not necessarily impossible) level. The kind of system implemented often depends on the acceptable threshold for theft. For example, keeping money in an inside shirt pocket increases the difficulty of theft above that necessary if the pocket was on a backpack, since unauthorized access is made sufficiently more difficult. Methods of theft evolve to decrease the difficulty of theft, increased by newer anti-theft systems. Because of evolution on both sides and the social aspect of theft, the threshold for theft is very dynamic and heavily dependent on the environment. Doors in quiet suburban neighbourhoods are often left unlocked, as the perceived thresholds for theft are very high.

c) Ease of use:

Security is often compromised through the lax application of theft-prevention practices and human nature in general. The average anti-theft device does not require any additional effort while using the secured item, without reducing the level of security. In practice, users of security systems may intentionally reduce the effectiveness of an anti-theft system to increase its usability (see passwords). For example, a home security system will usually be enabled and disabled with an easy-to-remember code such as "1111" or "123", instead of a more secure combination.

d) Modern features:

Modern and interesting or more precisely attractive features are always welcomed by users with open hands. so by creating an antitheft alarm of user attractive is very much a requirement. There should an room for up gradation about software, or new addition in programming, or anti-theft alarm device is operated through remote controller when user forgets on arm it and he/she is not nearby, there may be some other facilities like sending an message or email by using the concepts of internet of things. So by the discussion point of view we can see that our main motivation comes from the fact that if the user is satisfied or not, then only he or she will be willing to choose an anti-theft alarm system properly.

1.5 Need of the research:

In the modern era, the security of each and every household equipment is vital and so as the security of bi-cycle. Bi-cycles are widely used throughout the world and in our country it is almost used in every house. Bicycle theft is the biggest fear of any person. Stolen bike statistics are alarming in many places around the world. For example, in the UK nearly 400,000 bicycles are stolen annually while the global bicycle theft number is somewhere between 1.5 to 3 million. A big part of bicycle theft is unreported and remains unsolved. Generally, bi-cycles are stolen from house, streets, markets and parking lots. By the time, people understand that his bicycle has been stolen, the same is taken far away. Very often the security of bi-cycle relies solely on the manual lock. Securing the bi-cycle with a good lock does not mean that it will not be stolen. Also the manual locks sometimes damaged or people forget to lock and the thieves take advantage of the situation. To come out of the problem, there is need of putting of a security system in bi-cycle. Currently, apart from the manual locking system, other security system which have been developed works generally on internet and accordingly the same cannot fulfil the requirement in remote location. Also, these security systems are very costly. So, the bi-cycle companies are not able to implement such

as it increases the total cost of the same. So it is necessary to design the security system for a bi-cycle which is less costly & can easily be installed and also owner can put the same in his old bi-cycle easily.

Anti-theft alarm system is based solely on sensors which is the heart and soul of the system. It is the sensor that reads about the any kinds of movement that will trigger the alarm. Generally sensor collects data from the environment based on any trigger movement that processed through Arduino and triggers alarm which will alert the user. There are several limitations that have been identified and those limitations have opened the area of research. So the need of the researches are discussed below-

1. There can be some unwanted trigger movement to set the alarm, which can be eliminated by proper designing. There is also area to discuss about the threshold limit of sensor which is only triggered when there is a movement more than a prescribed value.

2. There should be a proper range use of alerting device that means a piezo buzzer range should be a proper value such that the user is able to detect it.

3. There are also some limitations about the power consumption of the components used. As high power consumption can reduce battery life drastically.

4. Limitations regarding putting Arduino to sleep and only wakes up if there is any trigger movement.

1.6 Literature Review:

There are several researches have been done on this field related to antitheft alarming device using different sensors and different techniques based on different need-

Holt and Young (1995) [1] Proposed that any kinds of anti-theft security alarm conforms to the appropriate British standards and related to NACOSS codes. Individual installations are certified, and records of each installation are kept centrally by NACOSS .And they have made a review of the effects of the installation of these alarms, drawing together information provided by the Home Office and the Police from their statistics, and from NACOSS records.

Lawrence and Pascoe (1998) [2] proposed a system of intruder alarm system to reduce the false alarming and also they have proposed an alternative strategy. They have also suggested that the use of IAS to prevent burglary and theft there is a substantial amount of false alarm going on so that they have proposed some counter measures for that.

Taryudi et al. (2006) [3] proposed that home safety remains a critical issues not only in metropolitan city but sub-urban areas, particularly for the people who does many activities outside of home. They have said that a proven strategy should be there to improve and make sure that security system and monitoring house environment remotely is needed. They have studied the design and developed an integrated home security and monitoring system using Internet of Things (IoT) by combined the Arduino nano and Node MCU ESP8266 as a controller. Their home security system involved RFID reader, numerical code to open the door and email notifications to users. The monitoring system used PIR sensor to detect the intruder, DHT-22 sensor to detect the room temperature and humidity, rain sensor to detect the rain, fire sensor to detect the stove's fire, and LDR sensors to monitor the light condition. Also, They have set up light bulbs and solenoid valves used as the actuators. The results of their study showed that the system can monitor the condition of the house and control the output of lights and solenoid valves remotely by using an application on the smartphone through internet connection.

Song et al. (2008) [4] said that vehicle theft rate is on higher side, thus tracking/alarming systems are being deployed with an increasing popularity. These systems however bear some limitations such as high cost, high false-alarm rate, and easy to be disabled. Their research describes the design, implementation and evaluation of a Sensor-network-based Vehicle Anti-Theft System (SVATS) to address above described limitations. In this system, the sensors installed in the vehicles that are parked within the same parking zone first forms a sensor network, then monitor and identify possible vehicle thefts by detecting unauthorised vehicle movement. When an unauthorized movement is detected, an alert will be reported to a base station in the parking area, which sends warning messages to the security office. This research focuses on the technical issues specific to the system such as topology management, theft detection, and intra-vehicle networking.

Xie et al. (2008) [5] described in their research that the use of use of rich inner resource of FPGA(Field Programmable Gate Arrays), a wireless alarm sending system is designed. It includes an encoder, FSK(Frequency Shift Keying) modulation and every channel's control circuits, which can decrease sound and increase reliability of the alarm system. The demodulation of received system is realized by an application specific integrated circuits MC3372. With the help of a single-chip microcomputer 89C51, the address decoder is also designed in the receiver. Adding to other anti-interference, the alarming system has effectively decreases the false alarm rate. This system can install up to 128 channel sending

devices. It can send an alarm to the host when there are some cases in stand-off areas, and the system will display on rotation multiple cases' area codes . The transmission distance is greater than 4Km in open zones. User can install more than one type sensors simultaneously, for example, smog sensor, combustible gas sensor or burglar sensor. Experiments show that the wireless alarm system has the strengths of high reliability, high anti-disturbance ability and low false-alarm rate. It can entirely meet the needs of alarm fireproofing and antitheft, etc.

Desii et al. (2008) [6] in their research have discussed about the modified pitch detection method is proposed that can be used for the detection of acoustical signals the frequency components of which vary according to specific periodic patterns. Usually, signals of this categories are produced by the alarm signals of an emergency vehicle. The detection of this type of signals can improve the safety guide for hearing people having ear problems by alerting the driver with a visual indication for example by putting on a light point on the map of a navigator device.

Poberaj (2008) [7] in their discussion have worked with MEMS devices are irreplaceable in automobile industries, computers, audio video technologies. This paper presents MEMS technology as a highly developed industry. Special attention is given to the capacitor accelerometers, how do they work and their applications. The research closes with quite extensively described MEMS fabrication process.

Wan (2009) [8] have discussed in their research papers an automobile anti-theft alarm system based on GSM communication network. The TC35 GSM module and Microcontroller is combined with the system, vibration sensor and speed sensor are used to achieve short message service (SMS) alarm and dual theft-proof of automobile. The drawback of traditional systems including less security and less alarming range is overcome, and the cost of this system is also very less, so it should have good application prospects in the future.

Bin feng (2010) [9] have discussed in their research papers that In the present global pollution and the greenhouse effect become more and more serious issues, it is an urgent problem of the world transportation to develop one kind of new non pollution, noiselessness the non-oil consumption transportation vehicle. The entry of electric bicycles make people see that there is some hope of solving the problem of city traffic pollution, the environmental protection and high efficiency electric bicycles are becoming more and more popular to the people. Combined with modern electronic technology, single-chip technology and intelligent

sensor technology, we carry on electric bicycle system software circuit design and development of innovation based on Hardware circuit for the electric bike problems. Designed one multifunctional protection instrument based on AT89C2051 which integrated includes sound and light monitor of battery, aided battery charger, speed control circuit and anti-theft devices. The multifunctional protection instrument of electric bicycle is a very good design, having some good controllability, high stability, and can save results automatically and automatic alarm.

Hui et al. (2010) [10] have discussed in their research a new kind of electronic and mechanical antitheft lock using digital code based on the technologies of DSP, serial communication and wireless data transmission. This lock has multiple functions with relatively good security, identification and alarm-giving. It is simple and has wide range of application and high reliability. Hardware frame and software flowchart of the system are presented as its function constitution principle and the development of mechanism have been specified.

V. Omprakash (2011) [11] in their research have discussed about the wireless home security with mobile. The major aim of their research is to investigate a cost effective solution that will provide controlling of home appliances remotely and will also enable home security against illegal intrusion when the home owner is not present. This system uses newly wireless communication platforms like Bluetooth, Infrared and Wi-Fi access to the system for security and automated appliance control. Home security has been a major issue where crime is increasing and everybody wants to take proper measures to prevent unauthorized intrusion. This particular system will works on different wireless communications and at least 3 of 10 mobiles uses for security purpose. The proposed system characteristics involve remote controlling of valuable goods, intrusion detection, system security and automatic-configuration such that system automatically adjusts the system settings on running hardware support check.

Brooks (2011) [12] has discussed about the whether the security agencies are on par with the Australian standard AS2201.They have conducted a survey of 451 domestic and commercial intruder alarm systems was completed across the Perth metropolitan area, Western Australia. The gathered data were evaluated against Australian Standard AS2201. The Australian Standard AS2201.1 required that intruder alarm control equipment shall be located within the alarmed area, located outside the entry / exit point and operate in dual end-of-line

supervision. But their study has found significant proportion of the intruder alarms measured did not comply with AS2201.1, with 17.52 per cent of panels located outside an alarmed area, 14.86 per cent panels located in the entry /exit point, 45.90 per cent of the panels not capable of dual end-of-line supervision and 58.75 per cent of the systems configured in single end-of-line supervision. These items do not follow some sections of the Australian Standard AS2201.1 and would appear to demonstrate systemic failure within this sector of the security industry. Further to these findings, the study made a number of final findings in an attempt to understand why such a level of non-compliance was found. Conclusions included a lack of industry-centred vocational training and education programme, limited industry self-regulation and supervision, restricted licensing regime, inappropriate legislation and not having a single federal approach to such matters. In addition, the introduction of a new performance based AS2201 standard may further decrease the ability to measure such non-compliance. However, no single reason discussed could be considered ineffective; rather, it is argued that all of these areas need to be addressed to significantly reduce the level of systemic non-compliance of intrusion or burgling alarms systems.

Jian-ming et al. (2012) [13] in their view they have discussed about automobile anti-theft systems mostly used static real-time detection and alarm at present, in their research they have designed an automobile anti-theft system based on GSM and GPS module. The system is developed on the basis of high speed mixed type single-chip C8051F120 and detect automobile being stolen or not and it sends an alarm to the automobile owner by vibration sensor. Automobile location can be obtained with the GPS module integrated in anti-theft system. The system can keep in touch with automobile owner through the GSM module, to monitor the safety and reliability of automobile with required level.

Olumide (2012) [14] have proposed in their research about the unauthorized access to residential and commercial buildings when the residents are far away from the access gate of the house. This system is a simple and reliable touch activated security system and uses sensor technology to revolutionize the standards of living. The system provides a best solution to most of the problems faced by house owners in their daily life. This system is also very cost effective. The system is divided into three units; the power supply unit which employs the use of both DC battery and mains supply to ensure constant power supply to the circuit, the trigger unit which is responsible for activating the alarm unit and designed to have much time and period and moderate sensitivity in order to reduce the rate of false alarm, and the alarm amplitude unit which main function is to produce amplitude alarm sound when

triggered by the trigger unit with the aim of producing a large audible sound that can alert the entire neighbourhood or scare an intruder away. The design of the system was achieved by considering some factors such as economy, availability of components and research materials, efficiency, compatibility and portability and also durability in the design process. The performance of the system after test has met design specifications. And for that purpose touch sensor has been used. The general operation of the system and performance is dependent on the presence of an intruder entering through the door and touching any part of the door. The overall system was constructed and tested and it work perfectly.

Victor (2012) [15] in their research have discussed an embedded system design with DTMF and a GSM to monitor and safeguard valuable things. Obviously it secures a car against theft burgling and it is also very prominent for other valuable goods. After it is activated, it automatically disables the car by disconnecting the ignition key supply from the car battery. This now makes it impossible for anybody so starts the car, let alone moving with it. In an attempt of theft through the car doors, the system sends text message to the car owner and at the same time starts up an alarm to notify nearby passers. This design popped out due to the increasing rate at which parked cars are being stolen especially, but with this design this parked car is being monitored irrespective of where it is parked, provided that there is GSM network coverage. From their research conducted, it was found that majority of the existing car security system uses only alarm sensor, and doesn't send text message to the car owner let alone of disabling the car. But with the use of GSM network, the owner is guaranteed that the car will send text message to his phone, and at the same time, have people around the car alerted of what is happening.

Biswa et al. (2013) [16] in their research paper have discussed about the PIR sensor based security system which reduces power consumption and memory space of the recording system. PIR sensor generally known as passive infrared radiation sensor detects changes in the infrared radiation of the warm blooded moving object. According to the change in infrared radiation, there will be a change in the voltages generated which was amplified and used to turn ON the webcam and lighting system through relay. Software was developed and installed in the computer to capture and record the video when the webcam gets turned ON. When an intruder comes within the range of the PIR sensor, it activates the lighting system and the webcam. The software detects the webcam connection; it will start to record and will save the video graphic image. Once the intruder moves out of range of the sensor, the webcam and light gets turn OFF. Thus the saves power consumption and the memory space

of the recording system as the lamp and webcam will only get turned ON when PIR sensors detects an object within its range. Consequently the system starts recording only when the webcam is turned ON; hence saving memory space.

Zungeru (2013) [17] has proposed a method against rapid increase in the crime related to theft, burgling related offences. Therefore he has tried to design a cheap and effective security system for buildings, cars, safes, doors and gates, so as to prevent burglars from having access to ones properties through the use of codes, therefore making electronic devices as locks. However, a modular approach was employed in the design in which the combination lock was divided into units and each unit designed separately before being coupled to form a whole functional system. And the general operation of the system and performance is dependent on the key combinations.

Reddy et al. (2013) [18] have studied about the issues related to security. They have also studied about the several security issues like gas leakage, theft burgling etc. They have also studied about the how to send SMS to owner about the intrusion burgling through GSM module.

Bangali and Shaligram (2013) [19] have studied about the security related issues. They have studied that there are two different types of ways through which we can solve security issues, one is using a camera that means whenever there is a movement in front of camera it will detect and sound an alarm and also sends an mail through IOT, second is movement detection through sensors and sending and SMS using GSM module.

Lee et al. (2013) [20] have studied about the multilevel home security system. MHSS is consist of a multilevel security system which is integral of different types sensor nodes as the input elements while the output elements react to the signal received from the input elements. The sensor nodes consist of an anti-theft alarm, presence detecting circuit and the break-in camera. They have also used an UART which is applied as the communication tool between the hardware and the computer. A graphic user interface (GUI) is developed and configured which enables the function of capturing images and sending emails. The captured images are delivered to the house owners and the police forces. The task is performed in order to prevent the invasion.

Anbazhagen et al. (2014) [21] have proposed about a locking and unlocking devices with the help of password. Due to the rapid development in the field of science and technology,

many more advancements have been made in automation and controlling the hardware can adopt this technique. This technique is also applicable to cars as well as home appliances. Two wheeler automobiles have several types of safety and security systems fuel supply open by password, ignition system starts by password and also head light activated by passwords.

Eseosa and Promise (2014) [22] have studied about the limitations of the alarm systems. These limitations in most cases result in high financial loss to properties and lives. There work involves design and construction of GSM based home security system for real time monitoring of intruders and anti-theft. It consist of intrusion detection sensors, (pressure, Smoke/Fire, Gas and PIR motion), wireless sensors, programmable microcontroller in embedded C language, regulated power supply unit, protects (circuit simulator), relays, GSM modem, mobile phone, data acquisition node and an interface program development. The design calculation and analysis was carried out before it was modelled, simulated in proteus electronic simulator environment. When the PIR finds intruders (in form of variation in temperature, gas leakage, pressure, etc), the relevant sensing device(s) respond and the microcontroller sends encoded alarm signal to the wireless sensor network established in home. The moment the alarm signal is received, it will send alarm short message to the users (owners of the building) through GSM network immediately.

Sulochana and Monahor Babu (2014) [23] have discussed about the delay between accidence and Responder to detect automatic vehicle accident in real time. This sense when a traffic accident is probable to occur and immediately notifies emergency situation occurred. Global positioning system technology this article designs and recognizes one kind of embedded wireless system. Their research focuses on the using accelerometer to detect any accident prone situations and also informing ambulance.

Samuel (2014) [24] have discussed about the microcontroller based security system with intruder display with automation. Their research focuses on tracking presence of intruder within the restricted place. Their Project will be based on microcontroller and other electronic design to achieve the above stated purposes. The interfacing medium will make use of parallel port. The sensors will detect any intruders and they will inform the owner. The hardware component depends mainly on microcontroller AT89S51.

Huan et al. (2014) [25] have discussed about the problems of fish being stolen frequently which effects agri products. They have tried to developed an anti-theft burgling alarm system with the help of Zigbee and GSM module. The system consisted of three parts: the anti-theft

terminal, communication network and monitoring centre. The anti-theft terminals communicated with monitoring centre by communication network. Except that anti-theft terminals were installed at the fixed point on the banks of the river, they were also installed on mobile patrol boat, which invested in the fishpond according to the preset trajectory to patrol the fishpond. This anti-theft wireless network is created on the basis of Zigbee network.

Fang et al. (2015) [26] have discussed about the remote anti-theft alarm system based on Zigbeemodule and GPRS. This system can detect the alarm information of the car with vibration sensor, pyro electric sensor and infrared sensor. When the sensor detects any alarm signal, the ZigBee node in sleep will be awakened and then directly send the alarm signal to the microcontroller chip S3C6410 in the control room of the parking lot through ZigBee wireless transceiver module.

Choudhury et al. (2015) [27] have invested their focus on a versatile anti –theft alarm system which is very cheap can be used by any individuals or corporates. The idea behind this project is to provide its users with a simple, fast and reliable system to get help during emergency situations. The device can be placed at any remote location which can be easily accessed by the user. It uses a microcontroller for system control, GSM technology for communication and sends SMS containing the emergency message and the GPS location of the sender.

Ashraf and Mamun (2015) [28] have discussed about vehicle theft that is a growing concern in most of the developing countries. There are some anti-theft systems developed in the past but there are certain problems associated with those those problems are analysed here. Those problems typically include false alarm, easy de activation, cost so they have created an easy reliable and economical device to help user with the integration with GSM and GPRS.

Nair et al. (2015) [29] have discussed about the rapid growth of technology and infrastructure which had mad our life more easier. The advent of technology has also increased the traffic hazards and the road accident take place frequently which causes huge loss of life and property because of the poor emergency facilities. Their research will provide an perfect solution to this draw back by using GSM, GPS and Accelerometer. In addition to, it also takes the precaution to prevent the accident by using alcohol sensor and Temperature sensor used to detect fire.

Fukate et al. (2015) [30] have proposed a system that will improve banking security. Fims are now facing a growing concern about the theft and burgling. They have developed an enterprise to improve banking locker security system which is based on RFID, GSM system and microcontroller devices. Here they have carried out some extra safety features in the existing scenario so the arrangement could become more secure than ever it would be. In this system they have used a very interesting feature like the addition of a MEMS technology. MEMS accelerometer is implemented using embedded microcontroller. Once the microcontroller senses any motion it will sound an alarm and asking for password to stop it.

Nwokye et al. (2015) [31] have discussed about a home security system based on GSM module. They have also investigated about the how peoples life style has changed and burgling chances are also increasing nowadays. Their final point is to build a SMS based anti-theft alarm system to detect and alert us of any wrongdoings. The circuit consist of an controller, receiver and sensor based circuit. A PIR sensor has also been used to detect unwanted intruder movement.

Divya et al. (2016) [32] have developed an anti-theft alarm system based on GPRS and GSM module and also they have tried to build a system to detect actual position of a car when stolen.The system contains GPS module, GSM modem, Infrared sensors, DTMF decoder IC MT8870DE, 8051 microcontroller, relay switch, vibration sensor, paint spray and high voltage mesh. GSM system is also installed in the vehicle for sending the information to the owner of the vehicle because GPS system can only receive the vehicle location information from satellites. In case of accident or any problem of the home owner it will send an alert to the relatives. The owner can lock or disable the system according to the will.

Dhonde et al. (2016) [33] have discussed about the software applications which are used to reduce energy consumption and time. Using electronics to good effect they have decided to build an automatic home safety and security system. They have mainly focussed on the busy families or someone having physical disability. Users can control home appliances or some other important things with electronics and prevent their theft.

Deshpande et al. (2016) [34] have discussed about the security system related to home a top most concern. Moreover, safe and secure residential space is the necessity of every individual as most of the family members are working. The home is left unattended for most of the day-time and home invasion crimes are at its peak as constantly monitoring of the home is difficult. Another reason for the need of home safety is specifically when the elderly person is

alone or the kids are with baby-sitter and servant. Home security system i.e. HomeOS is thus applicable and desirable for resident's safety and convenience. Thus they have tried to turned home a smart sector where we can say our appliances are relatively safer. They have also showed a graphical method of obtaining a best security system to implement in home appliances.

1.7 Objective and Scope of the research:

The primary objective of this study is to design and develop an alarm based security device to prevent theft of bi-cycle which is more affordable and flexible as far as installation and operation is concerned.

After reviewing past research papers extensively we have seen that there is a growing tendency to develop an alarm system which will provide an easy solution towards anti-theft or burgling. In the past research papers they have used PIR sensor to detect any intrusion or any burgling attempt. But there is a growing problem about the use of PIR sensor that any kinds of movement in front of it can trigger alarm. But accelerometer (Micro electrical mechanical system, MEMS) can be a potential solution under such circumstances. From review of the past literature it is observed that so far no research work has been reported on use of such accelerometer for developing anti-theft alarm system.

In view of the above, in the present research study a MPU6050 accelerometer will be used to detect any unauthorized movement and a threshold value such a way that it will trigger an alarm when a certain significant movement is detected. In order to achieve this objective of the research study has been framed as follows:

a) To study the relative advantage and dis-advantages of using MPU6050 in anti-theft /burglar alarm system over commonly used other sensors like PIR sensors, …etc which have been already used by previous researchers.
b) To study the possibility of integrating Micro-controllers with the MPU6050 accelerometer and to observe the characteristics of MPU6050 accelerometer in order to determine threshold limit of the alarm system on various cases.
c) To design the circuit and develop a programme for microcontroller and MPU6050 accelerometer based alarm system.
d) To design portable alarm box using CAD software and to fabricate the project box using 3D printing technology.

e) To carry out assembly of all the components in vero board inside the project box for real life applications.

Chapter 2

Microcontroller based alarm system

A microcontroller (MCU for microcontroller unit or UC for μ-controller) is a small computer on a single integrated circuit. In modern terminology, it is similar to, but less sophisticated than, a system on a chip (SoC); anSoC may include a microcontroller as one of its components. A microcontroller contains one or more CPUs (processor cores) along with memory and programmable input/output peripherals. Program memory in the form of ferroelectric RAM, NOR flash or OTP ROM is also often included on chip, as well as a small amount of RAM. Microcontrollers are designed for embedded applications, in contrast to the microprocessors used in computers or other general purpose applications consisting of various discrete chips.

Microcontrollers are used in automatically controlled products and devices, such as automobile engine control systems, implantable medical devices, remote controls, office machines, appliances, power tools, toys and other embedded systems. By reducing the size and cost compared to a design that uses a separate microprocessor, memory, and input/output devices, microcontrollers make it economical to digitally control even more devices and processes. Mixed signal microcontrollers are common, integrating analog components needed to control non-digital electronic systems. In the context of the internet of things, microcontrollers are an economical and popular means of data collection, sensing and actuating the physical world as edge devices.

2.1 Components required:

a) Arduino UNO
b) Accelerometer MPU 6050
c) Piezo Speaker
d) Push Buttons
e) LED’s
f) P channel and N channel MOSFET
g) 10k,47k,330 ohm Resistors

h) Capacitors(100nF)
i) 9V battery and battery clip
j) Vero board for compact circuit design.
k) Male And Female header pins
l) Soldering iron gun.
m) V-board cutter

2.2 Microcontrollers based system:

In our day to day life the role of micro-controllers has been immense. They are used in a variety of applications ranging from home appliances, FAX machines, Video games, Camera, Exercise equipment, Cellular phones musical Instruments to Computers, engine control, aeronautics, security systems and the list goes on. Back to security system, Robert Gaffigan (1997) discussed in his book entitle Home Security Projects about the usage of microcontroller to design and develop a simple security system for a single home. He made it very clear that programming was required to design a good security system. High level programming language makes it easier for human being to write the code of program, comparing to the low level language. Using only PIC Microcontroller or Programmable Integrated Controller, Robert Gaffigan (1997) was successfully designed a portable CO detector, pool alarm system, an early warning alarm system, and dog bark inhibitor system. He suggested that new user should start to learn programming using simulator. Programming using PIC to develop a security system required a good understanding of processor working principles. Microcontrollers usually contain from several to dozens of general purpose input/output pins (GPIO). GPIO pins are software configurable to either an input or an output state. When GPIO pins are configured to an input state, they are often used to read sensors or external signals. Configured to the output state, GPIO pins can drive external devices such as LEDs or motors, often indirectly, through external power electronics. Security system was created to produce a safe and sound environment for human being and personal properties. Security system mostly refers to electronic and computer controlled system which can monitor and scan any given area all the time automatically. Generally the microcontroller based security system consists of transmitter, receiver, phase locked loop and processing section.

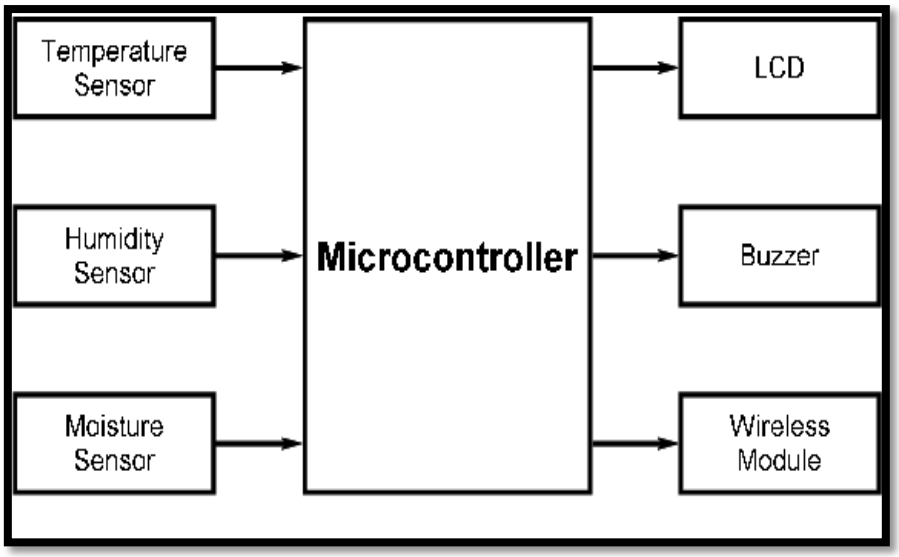


Fig 2.1: Concepts of Microcontroller based systems

2.3Difference between Microcontrollers and Microprocessors:

The microprocessors (such as 8086,80286,68000 etc.) contain no RAM, no ROM and no I/O ports on the chip itself. For this reason they are referred as general- purpose microprocessors. A system designer using general- purpose microprocessor must add external RAM, ROM, I/O ports and timers to make them functional. Although the addition of external RAM, ROM, and I/O ports make the system bulkier and much more expensive, they have the advantage of versatility such that the designer can decide on the amount of RAM, ROM and I/o ports needed to fit the task at hand. This is the not the case with microcontrollers. A microcontroller has a CPU (a microprocessor) in addition to the fixed amount of RAM, ROM, I/O ports, and timer is all embedded together on the chip: therefore, the designer cannot add any external memory, I/O, or timer to it. The fixed amount of on chip RAM, ROM, and number of I/O ports in microcontrollers make them ideal for many applications in which cost and space are critical. In many applications, for example a TV remote control, there is no need for the computing power of a 486 or even a 8086 microprocessor. In many applications, the space it takes, the power it consumes, and the price per unit are much more critical considerations than the computing power. These applications most often require some I/O operations to read signals and turn on and off certain bits. It is interesting to know that some microcontroller's manufactures have gone as far as integrating an ADC and other peripherals into the microcontrollers.

2.4 Microcontroller based embedded systems:

An embedded system is a controller programmed and controlled by a real-time operating system (RTOS) with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is *embedded* as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. Such as An PC contains or is connected to various embedded products such as the keyboard, printer, modem, disk controller, sound card, CD-ROM driver, mouse and so on. Each one of these peripherals has a microcontroller inside it that performs only one task. For example, inside every mouse there is a microcontroller to perform the task of finding the mouse position and sending it to the PC. Ninety-eight percent of all microprocessors manufactured are used in embedded systems. Modern embedded systems are often based on microcontrollers (i.e. CPUs with integrated memory or peripheral interfaces), but ordinary microprocessors (using external chips for memory and peripheral interface circuits) are also common, especially in more complex systems. In either case, the processor(s) used may be types ranging from general purpose to those specialized in certain class of computations or even custom designed for the application at hand. A common standard class of dedicated processors is the digital signal processor (DSP).Since the embedded system is dedicated to specific tasks, design engineers can optimize it to reduce the size and cost of the product and increase the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale. Embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations like traffic lights, factory controllers, and largely complex systems like hybrid vehicles, MRI, and avionics. Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure. In an embedded system, there is only one application software that is burned into ROM. Although microcontrollers are the preferred choice for many embedded systems, there are times that a microcontroller is inadequate for the task. For this reason, in many years the manufacturers for general-purpose microprocessors have targeted their microprocessor for the high end of the embedded market.

2.5 MEMS based sensors:

The advances in MEMS technologies and techniques means that manufacturers are now able to produce very capable MEMS sensors and devices, but many cannot be installed directly into an end application because they cannot survive the rigours of final assembly.

Conversely, conventional sensors can survive just about any assembly process and any application, but are perceived as being too big and too expensive. Hence the challenge for the manufacturers of MEMS sensors that are to be used in commercial products is to take the MEMS price and form factor, and package it into something able to withstand harsh environments.

2.5.1 MEMS technology:

MEMS stands for Micro electro-mechanical systems, is a technology used for the micro fabrication of electrical and mechanical components on a single wafer. This term is originated in the United States in 1990s, also referred as micro systems in Europe and labelled as micro machines in Japan. Prior to this technology was referred as silicon micro machining. MEMS technology provides a new functionality that previously could not be offered by the semiconductor devices.

In other words MEMS is a precision device in which mechanical parts and micro sensors along with the signal conditioning circuits are fabricated on a small piece of silicon. The letter S in the MEMS acronym indicates the systems which reflect that this technology contributes the creation of new system solutions. The elements that are integrated on the silicon chip using MEMS technology include micro sensors, mechanical structures, microelectronics and micro actuators as shown in figure. Micro sensors detect the changes of the system's environment by measuring thermal, chemical, electromagnetic, mechanical information, whereas these physical variables are processed by Microelectronics and then Micro actuators acts according to the changes of the environment.

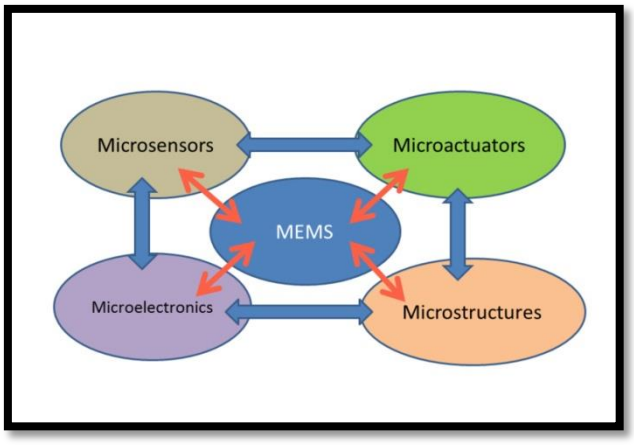


Fig 2.2 :Basic structures of MEMS

Some of the main factors that results a high level of interest in MEMS technology are:

a) Due to the pure crystalline structure with a silicon content of 99.999 percent, MEMS devices gives excellent mechanical characteristics which are resulting in no mechanical hysteresis or material fatigue.
b) It is possible to produce low cost and high-volume MSME devices with batch wafer processing technology. This high-volume production is very convenient with availability of cutting edge IC processing equipment's.
c) A lateral dimension to sub-micron level is greatly controlled.
d) . Availability of sophisticated devices for test and diagnosis and also high end software systems are available for design and simulation.
e) In the business side, MEMS devices assure large financial gains to the multiple emerging markets. MSME is selected as one of the three technologies expected to increase the growth of the economy in the 21st century by the Business Week in 1999.

2.5.2 MEMS Fabrication:

MEMS progress is resulted from a logical step in the silicon revolution and later with addition of micro machines allowed the integration of electronics with mechanical components to produce high performance, low cost and high functionality integrated micro systems. Silicon is the perfect material for fabricating micro sensors and micro actuators for different range of applications because it is a well-characterized material having properties like high thermal conductivity, lack of hysteresis, low bulk expansion, well-defined electrical properties with sensitive to strain, temperature, stress and other environmental factors, similar modulus of elasticity to that of steel, etc. In MEMS fabrication, silicon can be chemically etched into various shapes and associated thin-film materials such as poly silicon , aluminium and silicon nitride can be micro machined in batches into a vast variety of mechanical shapes and configurations. Various technologies are available for MEMS fabrication, two major technologies are usually employed are bulk micro machining and surface micro machining.

2.5.3 Various materials for MEMS manufacturing:

The fabrication of MEMS evolved from the process technology in semiconductor device fabrication, i.e. the basic techniques are deposition of material layers, patterning by photolithography and etching to produce the required shapes.

i. Silicon:

Silicon is the material used to create most integrated circuits used in consumer electronics in the modern industry. The economies of scale, ready availability of inexpensive high-quality materials, and ability to incorporate electronic functionality make silicon attractive for a wide variety ofMEMS applications. Silicon also has significant advantages engendered through its material properties. In single crystal form, silicon is an almost perfect Hooke an material, meaning that when it is flexed there is virtually no hysteresis and hence almost no energy dissipation. As well as making for highly repeatable motion, this also makes silicon very reliable as it suffers very little fatigue and can have service lifetimes in the range of billions to trillions of cycles without breaking.

ii. Polymers:

Even though the electronics industry provides an economy of scale for the silicon industry, crystalline silicon is still a complex and relatively expensive material to produce. Polymers on the other hand can be produced in huge volumes, with a great variety of material characteristics. MEMS devices can be made from polymers by processes such as injection moulding, embossing or stereo lithography and are especially well suited to microfluidic applications such as disposable blood testing cartridges.

iii. Metals:

Metals can also be used to create MEMS elements. While metals do not have some of the advantages displayed by silicon in terms of mechanical properties, when used within their limitations, metals can exhibit very high degrees of reliability. Metals can be deposited by electroplating, evaporation, and sputtering processes. Commonly used metals include gold, nickel, aluminium, copper, chromium, titanium, tungsten, platinum, and silver.

iv. Ceramics:

The nitrides of silicon, aluminium and titanium as well as silicon carbide and other ceramics are increasingly applied in MEMS fabrication due to advantageous combinations of material properties. AlN crystallizes in the quartzite structure and thus shows piezoelectric and piezoelectric properties enabling sensors, for instance, with sensitivity to normal and shear forces. TiN, on the other hand, exhibits a high electrical conductivity and large elastic modulus, making it possible to implement electrostatic MEMS actuation schemes with ultrathin membranes. Moreover, the high resistance of TiN against

bio corrosion qualifies the material for applications in biogenic environments and in biosensors.

2.5.4 Applications of MEMS technology:

Some common commercial applications of MEMS include:

i. Inkjet printers, which use piezoelectric or thermal bubble ejection to deposit ink on paper.

ii. Accelerometers in modern cars for a large number of purposes including airbag deployment and electronic stability control.

iii. Inertial Measurement Units (IMUs): MEMS Accelerometers and MEMS gyroscopes in remote controlled, or autonomous, helicopters, planes and multirotors (also known as drones), used for automatically sensing and balancing flying characteristics of roll, pitch and yaw. MEMS magnetic field sensor (magnetometer) may also be incorporated in such devices to provide directional heading. MEMS are also used in Inertial navigation systems (INSs) of modern cars, airplanes, submarines and other vehicles to detect yaw, pitch, and roll; for example, the autopilot of an airplane.

iv. Accelerometers in consumer electronics devices such as game controllers , personal media players / cell phones (virtually all smartphones, various HTC PDA models)and a number of Digital Cameras (various Canon Digital IXUS models). Also used in PCs to park the hard disk head when free-fall is detected, to prevent damage and data loss.

v. MEMS microphones in portable devices, e.g., mobile phones, head sets and laptops. The market for smart microphones includes smartphones, wearable devices, smart home and automotive applications.

vi. Precision temperature-compensated resonators in real-time clocks.

vii. Silicon pressure sensors e.g., car tire pressure sensors, and disposable blood pressure sensors.

viii. Displays e.g., the digital micro mirror device (DMD) chip in a projector based on DLP technology, which has a surface with several hundred thousand micro mirrors or single micro-scanning-mirrors also called micro scanners.

ix. Optical switching technology, which is used for switching technology and alignment for data communications.

x. Bio-MEMS applications in medical and health related technologies from Lab-On-Chip to Micro Total Analysis (biosensor, chemo sensor), or embedded in medical devices e.g. stents.

xi. Interferometry modulator display (IMOD) applications in consumer electronics (primarily displays for mobile devices), used to create interferometry modulation − reflective display technology as found in mirasol displays.

xii. Fluid acceleration such as for micro-cooling.

xiii. Micro-scale energy harvesting including piezoelectric, electrostatic and electromagnetic micro harvesters.

xiv. Micro machined ultrasound transducers.

2.6 Different types of Sensors:

There are different types of sensors that can be used for making of Anti-theft alarm system effectively. Below we have given comparative study of the different types of sensors-

Hermetically sealed reed switches:

The hermetically sealed reed switch is a very common type of two piece sensor that operates with an electrically conductive reed switch that is either normally opens or normally closed when under the influence of a magnetic field as in the case of proximity to the second piece which contains a magnet. When the magnet is moved away from the reed switch, the reed switch either closes or opens, again based on whether or not the design is normally open or normally closed. This action coupled with an electric current (typically at 12V DC) allows an alarm control panel to detect a fault on that zone or circuit. These types of sensors are very common and are found either wired directly to an alarm control panel, or they can typically be found in wireless door or window contacts as sub-components.

Passive infrared detectors:

The passive infrared (PIR) motion detector is one of the most common sensors found in household and small business environments. It offers affordable and reliable functionality. The term passive refers to the fact that the detector does not generate or radiate its own energy; it works entirely by detecting the heat energy given off by other objects. Strictly

speaking, PIR sensors do not detect motion; rather, they detect abrupt changes in temperature at a given point. As an intruder walks in front of the sensor, the temperature at that point will rise from room temperature to body temperature, and then back again. This quick change triggers the detection. PIR sensors may be designed to be wall- or ceiling-mounted, and come in various fields of view, from narrow-point detectors to 360-degree fields. PIRs require a power supply in addition to the detection signalling circuit.

Infrasound detectors:

The infrasound detector works by detecting infrasound, or sound waves at frequencies below 20 hertz. Sounds at those frequencies are inaudible to the human ear. Due to its inherent properties, infrasound can travel distances of many hundreds of kilometres. Infrasound signals can result from volcanic eruptions, earthquakes, gravity waves, opening and closing of doors, forcing windows to name a few. The entire infrasound detection system consists of the following components: a speaker (infrasound sensor) as a microphone input, an order-frequency filter, an analog to digital (A/D) converter, and finally an MCU, which is used to analyse the recorded signal. Each time a potential intruder tries enter into a house, she or he tests whether it is closed and locked, uses tools on openings, or/and applies pressure, and therefore he or she creates low-frequency sound vibrations. Such actions are immediately detected by the infrasound detector before the intruder breaks in. The primary purpose of such system is to stop burglars before they enter the house, to avoid not only theft, but vandalism. The sensitivity can be modulated depending on the size of a house and presence of animals.

Ultrasonic detectors:

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency. The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors:

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monocratic) for indoor applications, and separate housings (biostatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector, or Dual Tec brand or similar alarm. Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Compact surveillance radar:

Compact surveillance radar emits microwaves from a transmitter and detects any reflected microwaves. They are similar to microwave detectors but can detect the precise location of intruders in areas extending over hundreds of acres. With the capability of measuring range, angle, velocity, direction and size of the target, a CSR is able to pinpoint a precise GPS coordinate of an intruder. This target information is typically displayed on a map, user interface or situational awareness software that defines geographical alert zones or defences with different types of actions initiated depending on time of day and other factors. CSR is commonly used to protect outside the fence line of critical facilities such as electrical substations, power plants, dams, and bridges.

Photoelectric beams:

Photoelectric beam system detects the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an

effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a sealed condition whilst an intruder passes through, most systems use and detect a modulated light source.

Glass-break detection:

The glass-break detector may be used for internal perimeter building protection. Glass-break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass-break detectors, generally referred to as shock sensors, are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass-break detectors feel these shock frequencies and in turn generate an alarm condition. Window foil is a less sophisticated, mostly out dated detection method that involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electric current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

Motion sensors:

Motion sensors are devices that use various forms of technology to detect movement. The technology typically found in motion sensors to trigger an alarm includes infrared, ultrasonic, vibration and contact. Dual technology sensors combine two or more forms of detection in order to reduce false alarms as each method has its advantages and disadvantages. Traditionally motion sensors are an integral part of a home security system. These devices are typically installed to cover a large area as they commonly cover up to 40 ft with a 135° field of vision.

Vibration (shaker) or inertia sensors:

These devices are mounted on barriers and are used primarily to detect an attack on the structure itself. The technology relies on an unstable mechanical configuration that forms part

of the electrical circuit. When movement or vibration occurs, the unstable portion of the circuit moves and breaks the current flow, which produces an alarm. The technology of the devices varies and can be sensitive to different levels of vibration. The medium transmitting the vibration must be correctly selected for the specific sensor as they are best suited to different types of structures and configurations. A rather new and unproven type of sensor uses piezo-electric components rather than mechanical circuits, which can be tuned to be extremely sensitive to vibration.

- Advantages: Very reliable sensors, low false alarm rate, and mispriced.
- Disadvantages: Must be fence-mounted. The rather high price deters many customers, but its effectiveness offsets its high price. Piezo-electric sensors are a new technology with an unproven record as opposed to the mechanical sensor which in some cases has a field record in excess of 20 years.

Passive magnetic field detection:

This buried security system is based on the magnetic anomaly detection principle of operation. The system uses an electromagnetic field generator powered by two wires running in parallel. Both wires run along the perimeter and are usually installed about 5"/12 cm apart on top of a wall or about 12"/30 cm below ground. The wires are connected to a signal processor which analyses any change in the magnetic field. This kind of buried security system sensor cable could be embedded in the top of almost any kind of wall to provide a regular wall detection ability, or can be buried in the ground. They provide a very low false alarm rate, and have a very high chance of detecting real burglars. However, they cannot be installed near high voltage lines, or radar transmitters.

E-field:

This proximity system can be installed on building perimeters, fences, and walls. It also has the ability to be installed free standing on dedicated poles. The system uses an electromagnetic field generator powering one wire, with another sensing wire running parallel to it. Both wires run along the perimeter and are usually installed about 800 millimetres apart. The sensing wire is connected to a signal processor that analyses:

- amplitude change (mass of intruder),

- rate change (movement of intruder),
- pre-set disturbance time (time the intruder is in the pattern).

These items define the characteristics of an intruder and when all three are detected simultaneously, an alarm signal is generated. The barrier can provide protection from the ground to about 4 metres of altitude. It is usually configured in zones of about 200 metre lengths depending on the number of sensor wires installed.

- Advantage: concealed as a buried form.
- Disadvantages: expensive, short zones which mean more electronics (and thus a higher cost), and a high rate of false alarms as it cannot distinguish some pets from humans. In reality it does not work that well, as extreme weather may often cause false alarms.

Microwave barriers:

- Advantages: low cost, easy to install, invisible perimeter barrier, and unknown perimeter limits to the intruder.
- Disadvantages: extremely sensitive to weather; as rain, snow, and fog, for example, would cause the sensors to stop working, and need sterile perimeter line because trees and bushes or anything that blocks the beam would cause false alarm or lack of detection.

H-field:

This system employs an electro-magnetic field disturbance principle based on two unshielded (or 'leaky') coaxial cables buried about 10–15 cm deep and located at about 1 metre apart. The transmitter emits continuous Radio Frequency (RF) energy along one cable and the energy is received by the other cable. When the change in field strength weakens due to the presence of an object and reaches a pre-set lower threshold, an alarm condition is generated. The system is unobtrusive when it has been installed correctly, however care must be taken to ensure the surrounding soil offers good drainage in order to reduce nuisance alarms.

- Advantage: concealed as a buried form.

- Disadvantages: can be affected by RF noise, high rate of false alarms, difficult to install.

2.7 MPU 6050:

MPU 6050 is chosen based upon the past literature review by looking at the advantages and disadvantages of other sensors, cost effectiveness and compatibility with microcontroller programming. The MPU 6050 is a 6 DOF (degrees of freedom) or a six-axis IMU sensor, which means that it gives six values as output: three values from the accelerometer and three from the gyroscope. The MPU 6050 is a sensor based on MEMS (micro electro mechanical systems) technology. An accelerometer is a device that measures proper acceleration. Proper acceleration, being the acceleration (or rate of change of velocity) of a body in its own instantaneous rest frame, is not the same as coordinate acceleration, being the acceleration in a fixed coordinate system. For example, an accelerometer at rest on the surface of the Earth will measure acceleration due to Earth's gravity, straight upwards (by definition) of $g \approx 9.81\ m/s^2$. By contrast, accelerometers in free fall (falling toward the centre of the Earth at a rate of about $9.81\ m/s^2$) will measure zero.

Gyroscopes work on the principle of Coriolis acceleration. Imagine that there is a fork-like structure that is in a constant back-and-forth motion. It is held in place using piezoelectric crystals. Whenever you try to tilt this arrangement, the crystals experience a force in the direction of inclination. This is caused as a result of the inertia of the moving fork. The crystals thus produce a current in consensus with the piezoelectric effect, and this current is amplified. The values are then refined by the host microcontroller. Check this short video that explains how a works. Accelerometers have multiple applications in industry and science. Highly sensitive accelerometers are components of inertial navigation systems for aircraft and missiles. Accelerometers are used to detect and monitor vibration in rotating machinery. Accelerometers are used in tablet computers and digital cameras so that images on screens are always displayed upright. Accelerometers are used in drones for flight stabilisation. Coordinated accelerometers can be used to measure differences in proper acceleration, particularly gravity, over their separation in space; i.e., gradient of the gravitational field. This gravity is useful because absolute gravity is a weak effect and depends on local density of the Earth which is quite variable. Single- and multi-axis models of accelerometer are available to detect magnitude and direction of the proper acceleration, as a vector quantity, and can be used to sense orientation (because direction of weight changes), coordinate

acceleration, vibration, shock, and falling in a resistive medium (a case where the proper acceleration changes, since it starts at zero, then increases). Micro machined micro electromechanical systems (MEMS) accelerometers are increasingly present in portable electronic devices and video game controllers, to detect the position of the device or provide for game input.

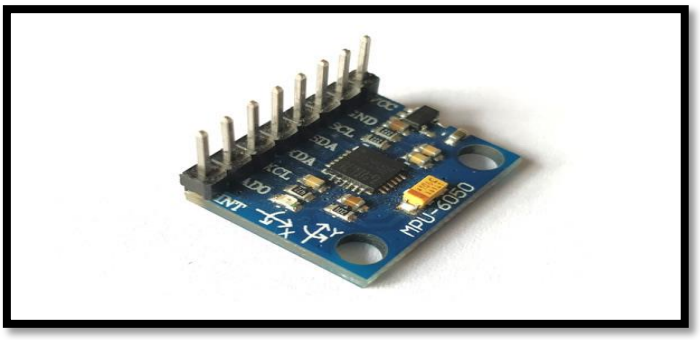


Fig 2.3: A MPU 6050 Module

2.7.1 Specifications:

MPU 6050 is a one type of accelerometer or another type of motion sensing device. By combining a MEMS 3-axis gyroscope and a 3-axis accelerometer on the same silicon die together with an on board Digital Motion Processor capable of processing complex 9-axis Motion Fusion algorithms, the MPU-6050 does away with the cross-axis alignment problems that can creep up on discrete parts.

Specifications of MPU 6050 include the followings:

a) Chip: MPU-6050
b) Power supply: 3~5V On board regulator
c) Communication mode: standard IIC communication protocol
d) Chip built-in 16bit AD converter, 16bit data output
e) Gyroscopes range: +/- 250 500 1000 2000 degree/sec
f) Acceleration range: +/- 2g, +/- 4g, +/- 8g, +/- 16g
g) Pin pitch: 2.54mm
h) Great for DIY projects

2.7.2 Pin configurations:

General pin configurations of MPU 6050 are showing below. Through these pins MPU 6050 is interconnected to arduino board. After connections are made with the arduino boards and necessary programme uploading the behaviour of MPU 6050 can be seen on Arduino IDE monitor.

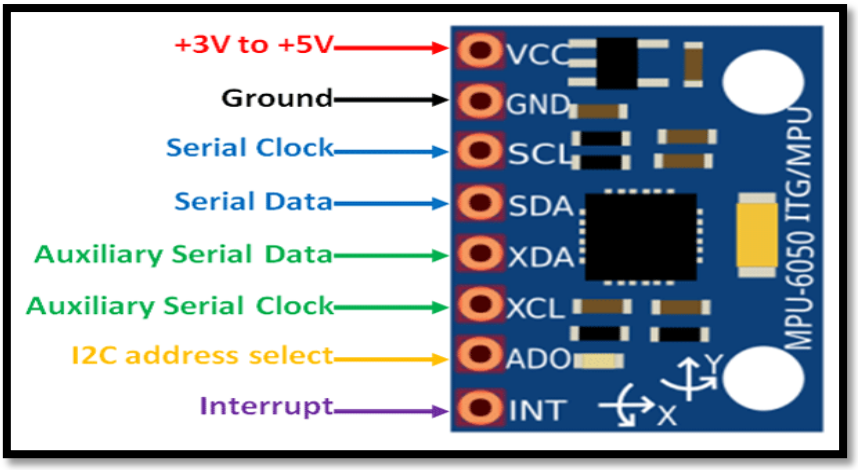


Fig 2.4: Pin configurations of MPU 6050

2.8 ARDUINO:

Arduino is a tool for making computers that can sense and control more of the physical world than desktop computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board.

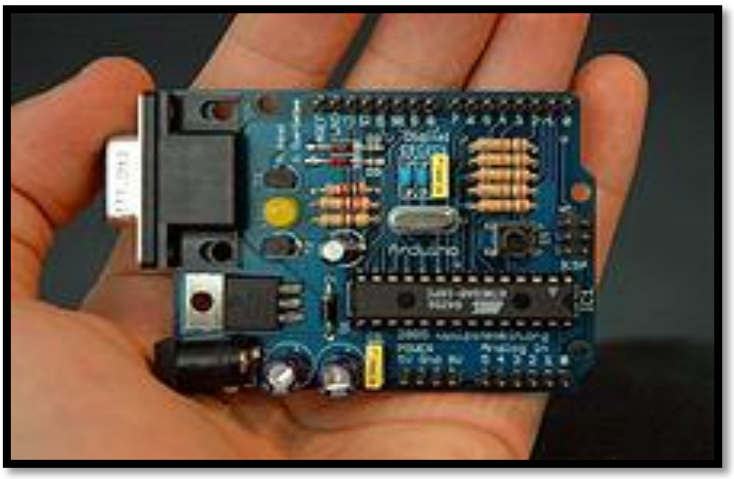


Fig 2.5 : Initial picture of Arduino

Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical outputs. Arduino projects can be stand-alone, or they can be communicating with software running on your computer (e.g. Flash, Processing, MAX-MSP.) The boards can be assembled by hand or purchased preassembled; the open-source IDE can be downloaded for free. The Arduino programming language is an implementation of Wiring, a similar physical computing platform, which is based on the Processing multimedia programming environment. Arduino is a popular open-source single-board microcontroller, descendant of the open-source Wiring platform designed to make the process of using electronics in multidisciplinary projects more accessible. The hardware consists of a simple open hardware design for the Arduino board with an Atmel AVR processor and on-board input/output support. The software consists of a standard programming language compiler and the boot loader that runs on the board. Arduino hardware is programmed using a Wiring-based language (syntax and libraries), similar to C++ with some slight simplifications and modifications, and a Processing-based integrated development environment. Arduino is an open-source electronics platform based on easy-to-use hardware and software. It's intended for anyone making interactive projects. Arduino can take the input from many sensors attached to it & can give the output to many lights, motors etc. There is no prerequisite knowledge of Advance electronics for operating Arduino. All you should know is basic electronics and C programming language.

Arduino platform mainly contains a Hardware Board called Arduino Board & software Arduino IDE to program it. Other external hardware like Sensor Modules, Motors, lights etc. could be attached with the board.

Arduino Boards:

a) Arduino UNO.
b) Arduino MEGA.
c) Arduino MINI.
d) Arduino DUE.
e) Arduino YUN.
f) Arduino Lily pad.

The most common Board used is Arduino UNO. “UNO" means one in Italian and was chosen to mark the release of Arduino Software (IDE) 1.0. The Uno board and version 1.0 of

Arduino Software (IDE) were the reference versions of Arduino, now evolved to newer releases.

2.8.1 Reason behind selecting Arduino:

There are many other microcontrollers and microcontroller platforms available for physical computing. Parallax Basic Stamp, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

a) **Inexpensive:** Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50
b) **Cross-platform:** The Arduino software runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
c) **Simple, clear programming environment:** The Arduino programming environment is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with the look and feel of Arduino.
d) **Open source and extensible software:** The Arduino is based on Atmel's ATMEGA8 and ATMEGA168microcontrollers. The plans for the modules are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.
e) **Open source and extensible hardware:** The Arduino is based on Atmel's ATMEGA8 and ATMEGA168microcontrollers. The plans for the modules are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

2.8.2 Arduino Hardware:

Arduino is open-source hardware. The hardware reference designs are distributed under a Creative Commons Attribution Share-Alike 2.5 license and are available on the Arduino website. Layout and production files for some versions of the hardware are also available.

Although the hardware and software designs are freely available under copy left licenses, the developers have requested the name Arduino to be exclusive to the official product and not be used for derived works without permission. The official policy document on use of the Arduino name emphasizes that the project is open to incorporating work by others into the official product. Several Arduino-compatible products commercially released have avoided the project name by using various names ending in *-duino*. Most Arduino boards consist of an Atmel 8-bit AVR microcontroller (ATmega8,ATmega168, ATmega328, ATmega1280, ATmega2560) with varying amounts of flash memory, pins, and features. The 32-bit Arduino Due, based on the Atmel SAM3X8E was introduced in 2012. The boards use single or double-row pins or female headers that facilitate connections for programming and incorporation into other circuits. These may connect with add-on modules termed shields. Multiple and possibly stacked shields may be individually addressable via an I²C serial bus. Most boards include a 5 V linear regulator and a 16 MHz crystal oscillator or ceramic resonator. Some designs, such as the LilyPad, run at 8 MHz and dispense with the on board voltage regulator due to specific form-factor restrictions. Arduino microcontrollers are pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory. The default boot loader of the Arduino UNO is the opti boot loader. Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor–transistor logic(TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header. Other variants, such as the Arduino Mini and the unofficial Board arduino, use a detachable USB-to-serial adapter board or cable, Bluetooth or other methods. When used with traditional microcontroller tools, instead of the Arduino IDE, standard AVR in-system

programming (ISP) programming is used. The Arduino board exposes most of the microcontroller's I/O pins for use by other circuits. The current Uno provide 14 digital I/O pins, six of which can produce pulse-width modulated signals, and six analog inputs, which can also be used as six digital I/O pins. These pins are on the top of the board, via female 0.1-inch (2.54 mm) headers. Several plug-in application shields are also commercially available. The Arduino Nano, and Arduino-compatible Bare bones Board and Board arduino boards may provide male header pins on the underside of the board that can plug into solder less breadboards.

Many Arduino-compatible and Arduino-derived boards exist. Some are functionally equivalent to an Arduino and can be used interchangeably. Many enhance the basic Arduino by adding output drivers, often for use in school-level education, to simplify making buggies and small robots. Others are electrically equivalent but change the form factor, sometimes retaining compatibility with shields, sometimes not. Some variants use different processors, of varying compatibility.

2.8.3 Arduino Software:

A program for Arduino hardware may be written in any programming language with compilers that produce binary machine code for the target processor. Atmel provides a development environment for their 8-bit AVR and 32-bit ARM Cortex-M based microcontrollers: AVR Studio (older) and Atmel Studio (newer).

a) IDE:

The Arduino integrated development environment (IDE) is a cross-platform application (for Windows, macOS, Linux) that is written in the programming language Java. It originated from the IDE for the languages Processing and Wiring. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting, brace matching, and syntax highlighting, and provides simple *one-click* mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions and a hierarchy of operation menus. The source code for the IDE is released under the GNU General Public License, version 2.

The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions,

for starting the sketch and the main program loop, that are compiled and linked with a program stub *main()* into an executable cyclic executive program with the GNU tool chain, also included with the IDE distribution. The Arduino IDE employs the program *avrdude* to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware.

b) Sketch:

A sketch is a program written with the Arduino IDE Sketches is saved on the development computer as text files with the file extension **.ino**. Arduino Software (IDE) pre-1.0 saved sketches with the extension **.pde**.

A minimal Arduino C/C++ program consists of only two functions:

`setup ()`: This function is called once when a sketch starts after power-up or reset. It is used to initialize variables, input and output pin modes, and other libraries needed in the sketch. `loop()`: After `setup()` function exits (ends), the `loop()` function is executed repeatedly in the main program. It controls the board until the board is powered off or is reset.

2.8.4 Arduino UNO:

Arduino is an open-source computer hardware and software company, project and user community that designs and manufactures microcontroller-based kits for building digital devices and interactive objects that can sense and control the physical world. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The board has 14 Digital pins, 6 Analog pins, and programmable with the Arduino IDE (Integrated Development Environment) via a type B USB cable. It can be powered by a USB cable or by an external 9 volt battery, though it accepts voltages between 7 and 20 volts. It is also similar to the Arduino Nano and Leonardo. The hardware reference design is distributed under a Creative Commons Attribution Share-Alike 2.5 license and is available on the Arduino website. Layout and production files for some versions of the hardware are also available. "Uno" means one in Italian and was chosen to mark the release of Arduino Software (IDE) 1.0. The Uno board and version 1.0 of Arduino Software (IDE) were the reference versions of Arduino, now evolved to newer releases. The Uno board is the first in a series of USB Arduino boards, and the reference model for the Arduino platform. The ATmega328 on the

Arduino Uno comes preprogramed with a boot loader that allows uploading new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol. The Uno also differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it uses the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. The first Arduino was introduced in 2005, aiming to provide an inexpensive and easy way for novices and professionals to create devices that interact with their environment using sensors and actuators. Common examples of such devices intended for beginner hobbyists include simple robots, thermostats, and motion detectors.

2.8.4.1 Technical specifications:

i. Microcontroller: Microchip ATmega328P
ii. Operating Voltage: 5 Volts
iii. Input Voltage: 7 to 20 Volts
iv. Digital I/O Pins: 14 (of which 6 provide PWM output)
v. Analog Input Pins: 6
vi. DC Current per I/O Pin: 20 mA
vii. Flash Memory: 32 KB of which 0.5 KB used by boot loader
viii. SRAM: 2 KB
ix. EEPROM: 1 KB
x. Clock Speed: 16 MHz
xi. Length: 68.6 mm
xii. Width: 53.4 mm
xiii. Weight: 25 g

2.8.4.2 Pin Description:

In the figure we have discussed about the description of pins that comprises a Arduino UNO board. There positional and descriptive details are shown in the figure-

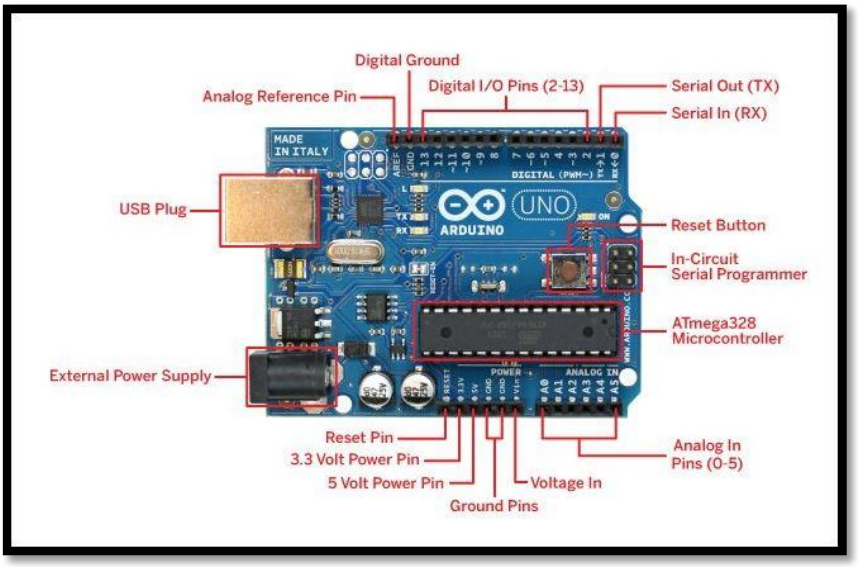


Fig 2.6: Arduino UNO

Vcc	Provides power to the MODULE
GND	Connect to Ground system
SCL	Used to provide clock pulse for I2C communications
SDA	Used for transferring data
XDA	Can be used for interfacing other I2C modules
XCL	Can be used to interface other I2C modules
AD0	If more than one MPU6050 is used a single MCU, then this pin can be used to vary the address
INT	Interrupt pin to indicate that data is available for MCU to read.

2.8.4.3 General pin functions:

i. **LED**: There is a built-in LED driven by digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.

ii. **VIN**: The input voltage to the Arduino/Genuino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated

power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.

iii. **5V**: This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 - 20V), the USB connector (5V), or the VIN pin of the board (7-20V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage the board.

iv. **3V3**: A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.

v. **GND**: Ground pins.

vi. **IOREF**: This pin on the Arduino/Genuino board provides the voltage reference with which the microcontroller operates. A properly configured shield can read the IOREF pin voltage and select the appropriate power source or enable voltage translators on the outputs to work with the 5V or 3.3V.

vii. **Reset**: Typically used to add a reset button to shields which block the one on the board.

2.8.4.4 Special pin functions:

Each of the 14 digital pins and 6 Analog pins on the Uno can be used as an input or output, using pinMode(),digitalWrite(), and digitalRead() functions. They operate at 5 volts. Each pin can provide or receive 20 mA as recommended operating condition and has an internal pull-up resistor (disconnected by default) of 20-50k ohm. A maximum of 40mA is the value that must not be exceeded on any I/O pin to avoid permanent damage to the microcontroller. The Uno has 6 analog inputs, labelled A0 through A5, each of which provide 10 bits of resolution (i.e. 1024 different values). By default they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analogReference() function.

In addition, some pins have specialized functions:

i. **Serial** / UART: pins 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data. These pins are connected to the corresponding pins of the ATmega8U2 USB-to-TTL Serial chip.

ii. **External Interrupts**: pins 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value.

iii. **PWM** (**P**ulse **W**idth **M**odulation): 3, 5, 6, 9, 10, and 11 Can provide 8-bit PWM output with the analogWrite() function.

iv. **SPI** (**S**erial **P**eripheral **I**nterface): 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication using the SPI library.

v. **TWI** (**T**wo **W**ire **I**nterface) / I²C: A4 or SDA pin and A5 or SCL pin. Support TWI communication using the Wire library.

vi. **AREF** (**A**nalog **REF**erence): Reference voltage for the analog inputs.

2.9 ATMEGA 328P:

The computer on one hand is designed to perform all the general purpose tasks on a single machine like you can use a computer to run a software to perform calculations or you can use a computer to store some multimedia file or to access internet through the browser, whereas the microcontrollers are meant to perform only the specific tasks, for e.g., switching the AC off automatically when room temperature drops to a certain defined limit and again turning it ON when temperature rises above the defined limit. There are number of popular families of microcontrollers which are used in different applications as per their capability and feasibility to perform the desired task, most common of these are 8051, AVR and PIC microcontrollers. In this we will introduce you with AVR family of microcontrollers. The ATmega328 is a single-chip microcontroller created by Atmel in the mega AVR family (later Microchip Technology acquired Atmel in 2016). It has a modified Harvard architecture 8-bit RISC processor core.

2.9.1 History of AVR:

AVR was developed in the year 1996 by Atmel Corporation. The architecture of AVR was developed by Alf-EgilBogen and VegardWollan. AVR derives its name from its developers and stands for Alf-EgilBogenVegardWollan RISC microcontroller, also known as Advanced Virtual RISC.

AVR microcontrollers are available in three categories:

a) **Tiny AVR**– Less memory, small size, suitable only for simpler applications.
b) **Mega AVR**– These are the most popular ones having good amount of memory (up-to 256 KB), higher number of in-built peripherals and suitable for moderate to complex applications.

c) **Xmega AVR**– Used commercially for complex applications, which require large program memory and high speed.

2.9.2 Features:

i. RISC Architecture with CISC Instruction set.
ii. Powerful C and assembly programming.
iii. Scalable
iv. Same powerful AVR microcontroller core.
v. Low power consumption
vi. Both digital and analog input and output interfaces.

2.9.3 Pin Description:

The Atmel ATmega48/88/328 is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega48/88/328 achieves throughputs approaching 1 MIPS per MHz allowing the system designed to optimize power consumption versus processing speed.

The Atmel ATmega48/88/328 provides the following features: 4K/8K/16K bytes of In-System Programmable Flash with Read-While-Write capabilities, 256/512/512 bytes EEPROM, 512/1K/1K bytes SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible Timer/Counters with compare modes, internal and external interrupts, a serial programmable USART, a byte-oriented 2-wire Serial Interface, an SPI serial port, a 6-channel 10-bit ADC (8 channels in TQFP and QFN/MLF packages), a programmable Watchdog Timer with internal Oscillator, and five software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, USART, 2-wire Serial Interface, SPI port, and interrupt system to continue functioning. The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or hardware reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except asynchronous timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the crystal/resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption. The ATmega48, ATmega88 and ATmega328 differ only in memory sizes, boot loader support,

and interrupt vector sizes.ATmega88 and ATmega328 support a real Read-While-Write Self-Programming mechanism. There is a separate Boot Loader Section, and the SPM instruction can only execute from there. InATmega48, there is no Read-While-Write support and no separate Boot Loader Section. The SPM instruction can execute from the entire Flash.

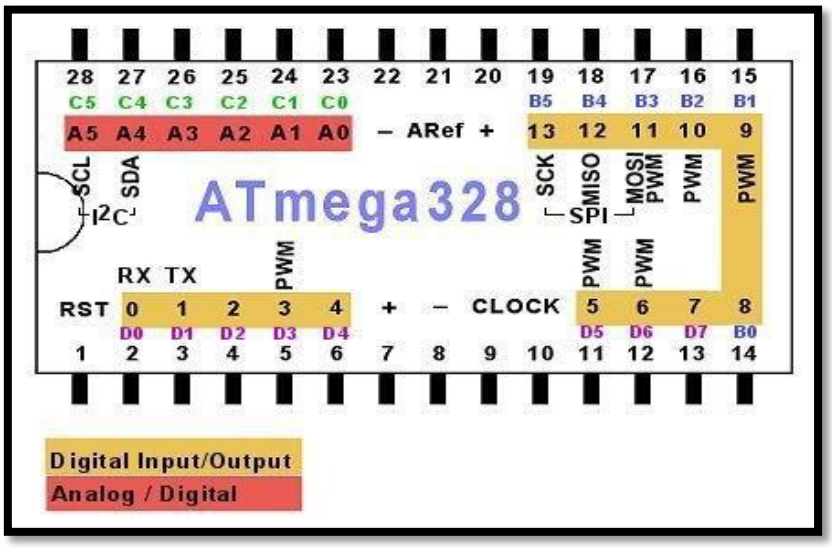


Fig 2.7: ATMEGA Pin Description

The ATmega48PA/88PA/168PA/328P is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture (RISC, or Reduced Instruction Set Computer**)** is a type of microprocessor architecture that utilizes a small, highly-optimized set of instructions). By executing powerful instructions in a single clock cycle, the ATmega48PA/88PA/168PA/328P achieves throughputs approaching 1 MIPS per MHz allowing the system designed to optimize power consumption versus processing speed. The AVR (Advanced Virtual RISC) core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers. The ATmega48PA/88PA/168PA/328P provides the following features: 4/8/16/32K bytes of In System Programmable Flash with Read-While-Write capabilities, 256/512/512/1K bytes EEPROM, 512/1K/1K/2K bytes SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible Timer/Counters with compare modes, internal and external interrupts, a serial programmable USART, a byte-oriented 2-wire Serial Interface, an SPI serial port, a 6-channel 10-bit ADC , a programmable Watchdog Timer with internal Oscillator, and five software selectable power

saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, USART, 2-wire Serial Interface, SPI port, and interrupt system to continue functioning.

The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or hardware reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping.

The ADC Noise Reduction mode stops the CPU and all I/O modules except asynchronous timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the crystal/resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption.

The device is manufactured using Atmel's high density non-volatile memory technology. The On-chip ISP Flash allows the program memory to be reprogrammed In-System through an SPI serial interface, by a conventional non-volatile memory programmer, or by an On-chip Boot program running on the AVR core. The Boot program can use any interface to download the application program in the Application Flash memory.

2.9.4 Internal Description:

Power:

The Arduino/Genuino Uno board can be powered via the USB connection or with an external power supply. The power source is selected automatically. External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted inthe GND and Vin pin headers of the POWER connector. The board can operate on an external supply from 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may become unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts.

The power pins are as follows:

i. **Vin. :**The input voltage to the Arduino/Genuino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.

ii. **5V.:**This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 - 12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board. We don't advise it.

iii. **3V3**.: A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.

iv. **GND. :**Ground pins.

v. **IOREF**.: This pin on the Arduino/Genuino board provides the voltage reference with which the microcontroller operates. A properly configured shield can read the IOREF pin voltage and select the appropriate power source or enable voltage translators on the outputs to work with the 5V or 3.3V.

Memory

The ATmega328 has 32 KB (with 0.5 KB occupied by the bootloader). It also has 2 KB of SRAM and 1 KB of EEPROM (which can be read and written with the EEPROM library).

Input and Output

Each of the 14 digital pins on the Uno can be used as an input or output, using pinMode(),digitalWrite(), and digitalRead() functions. They operate at 5 volts. Each pin can provide or receive 20 mA as recommended operating condition and has an internal pull-up resistor (disconnected by default) of 20-50k ohm. A maximum of 40mA is the value that must not be exceeded on any I/O pin to avoid permanent damage to the microcontroller.

In addition, some pins have specialized functions:

i. **Serial**: 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data. These pins are connected to the corresponding pins of the ATmega8U2 USB-to-TTL Serial chip.

ii. **External Interrupts**: 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attachInterrupt() function for details.

iii. **PWM**: 3, 5, 6, 9, 10, and 11. Provide 8-bit PWM output with the analogWrite() function.

iv. **SPI**: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication using the SPI library.

v. **LED**: 13. There is a built-in LED driven by digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.

vi. **TWI**: A4 or SDA pin and A5 or SCL pin. Support TWI communication using the Wire library.

The Uno has 6 analog inputs, labeled A0 through A5, each of which provide 10 bits of resolution (i.e. 1024 different values). By default they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analogReference() function.

There are a couple of other pins on the board:

i. **AREF**.: Reference voltage for the analog inputs. Used with analogReference().

ii. **Reset**. : Bring this line LOW to reset the microcontroller. Typically used to add a reset button to shields which block the one on the board.

2.10 Push buttons:

A push-button (also spelled pushbutton) or simply button is a simple switch mechanism for controlling some aspect of a machine or a process. Buttons are typically made out of hard material, usually plastic or metal. The surface is usually flat or shaped to accommodate the human finger or hand, so as to be easily depressed or pushed. Buttons are most often biased switches, although many un-biased buttons (due to their physical nature) still require a spring to return to their un-pushed state. Terms for the "pushing" of a button include pressing, depressing, mashing, slapping, hitting, and punching.

Fig 2.8 Different types of Push buttons

2.11 Concepts of LED and Capacitors:

In electronics, an LED circuit or LED driver is an electrical circuit used to power a light-emitting diode (LED). The circuit must provide sufficient current to light the LED at the required brightness, but must limit the current to prevent damaging the LED. The voltage drop across an LED is approximately constant over a wide range of operating current; therefore, a small increase in applied voltage greatly increases the current. Very simple circuits are used for low-power indicator LEDs. More complex, current source circuits are required when driving high-power LEDs for illumination to achieve correct current regulation.

A capacitor is a passive two-terminal electronic component that stores electrical energy in an electric field. The effect of a capacitor is known as capacitance. While some capacitance exists between any two electrical conductors in proximity in a circuit, a capacitor is a component designed to add capacitance to a circuit. The capacitor was originally known as a condenser or condensator The original name is still widely used in many languages, but not commonly in English.

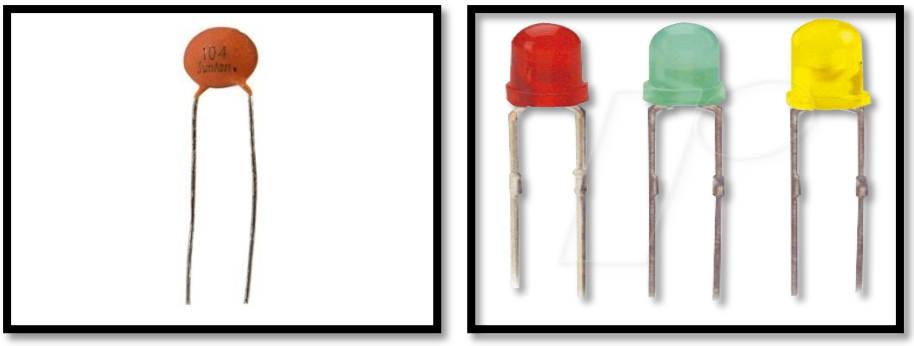


Fig 2.9 Capacitors and LED's

2.12 Vero board:

Veroboard is a brand of stripboard, a pre-formed circuit board material of copper strips on an insulating bonded paper board which was originated and developed in the early 1960s by the Electronics Department of Vero Precision Engineering Ltd (VPE). It was introduced as a general-purpose material for use in constructing electronic circuits - differing from purpose-designed printed circuit boards (PCBs) in that a variety of electronic circuits may be constructed using a standard wiring board. The first single-size Vero board product was the forerunner of the numerous types of prototype wiring board which, with worldwide use over five decades, have become known as strip board. The generic terms 'Vero board' and 'strip board' are now taken to be synonymous.

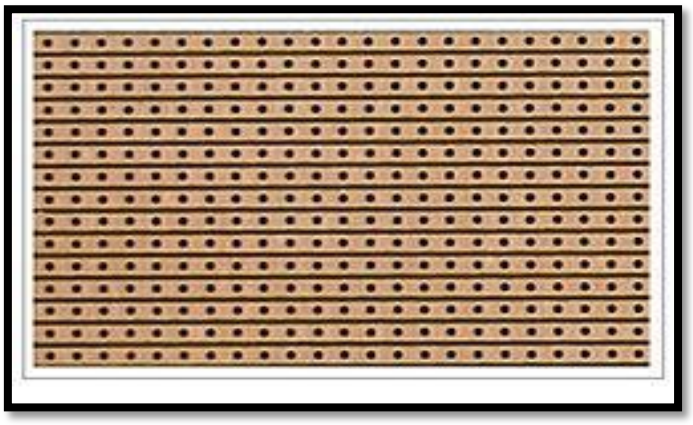


Fig 2.10 :Simple Vero Board

2.13 Piezo Buzzer:

A piezoelectric speaker (also known as a piezo bender due to its mode of operation, and sometimes colloquially called a "piezo", buzzer, crystal loudspeaker or beep speaker) is a loudspeaker that uses the piezoelectric effect for generating sound. The initial mechanical motion is created by applying a voltage to a piezoelectric material, and this motion is typically converted into audible sound using diaphragms and resonators. Compared to other speaker designs piezoelectric speakers are relatively easy to drive; for example they can be connected directly to TTL outputs, although more complex drivers can give greater sound intensity. Typically they operate well in the range of 1-5kHz and up to 100kHz in ultrasound applications. Piezoelectric speakers are frequently used to generate sound in digital quartz watches and other electronic devices, and are sometimes used as tweeters in less-expensive speaker systems, such as computer speakers and portable radios. They are also used for producing ultrasound in sonar systems. Piezoelectric speakers have several advantages over conventional loudspeakers: they are resistant to overloads that would normally destroy most high frequency drivers, and they can be used without a crossover due to their electrical properties. There are also disadvantages: some amplifiers can oscillate when driving capacitive loads like most piezoelectric, which results in distortion or damage to the amplifier. Additionally, their frequency response, in most cases, is inferior to that of other technologies, especially with regards to bass and midrange. This is why they are generally used in applications where volume and high pitch are more important than sound quality.

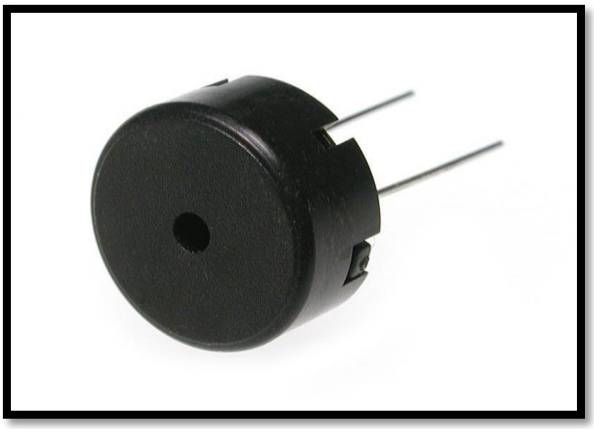


Fig 2.11: Piezo Buzzer

2.14 Development of Alarm based security system:

So far we have discussed about the components required to make a frame work for the development of sensor based anti-theft alarm system. Now we will see how actually the anti-theft alarm system is being made in to reality. First we will see about the circuit design which had helped us to implement our project, then we will discuss about the circuit development on vero board, then uploading the intended programme to Arduino UNO. Step by step the discussion on the project is given below-

a) **Circuit diagram:** The circuit diagram that we have followed is given below-

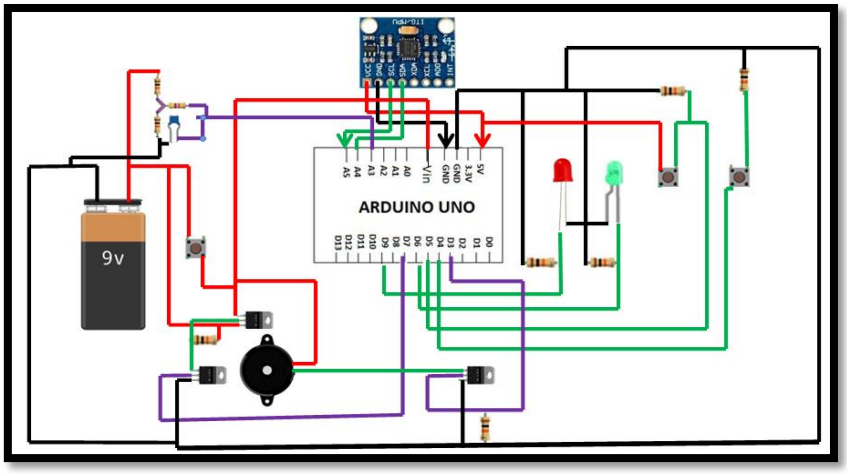


Fig 2.12: Representative Circuit Diagram

b) **Description of Circuit diagram:** In fig 2.12, the circuit diagram shows Arduino UNO as an interface to detect the programmed information. With the Arduino we have attached accelerometer MPU6050 and the pins used in Arduino are-

i. Vcc----5V

ii. GND-----GND

iii. SCL------A5

iv. SDA------A4

Then there is two LED's Green and Red for status report and low battery consumption indication, which are integral with 10K resistors to protect from the higher voltages. There is three buttons one of them is used in conjunction with a P-channel MOSFET to switch on the arduino. Other two buttons are used to give correct password in order to stop the buzzer after theft is detected successfully. Two passcode buttons have occupied arduino digital pin '4' and '5' and power on to arduino switch occupied arduino Vin port. P-channel MOSFET is

generally used on higher side of power supply, and N-channel MOSFET is generally used on the lower supply of power supply. N-channel are well-suited for when voltage is pulled down through a load while P-channel are good for when voltage is pulled up through a load. Black lines are set up for ground terminal. The piezoelectric buzzer is used here is in conjunction with the one N-channel MOSFET and another port is with the 9V battery power supply. One 100nF capacitor, one 41k resistor in conjunction with two 10k resistor is used to save the circuit form higher voltage supply.

c) **Step wise circuit Development on V-board:** Now we shall shift our focus on implementing the circuit shown above on vero board in order to shrink the circuit to make it industry friendly and also make it possible to fit inside customized project box. Below are the steps taken towards our intentions-

i. First of all to implement our circuit on v-board we have purchased a copper plate base v-board which is pretty easy to solder. In our v-board the square circles do not have any internal connections which is pretty much easier to connection. Fig 2.13 shows two types of Vero board-

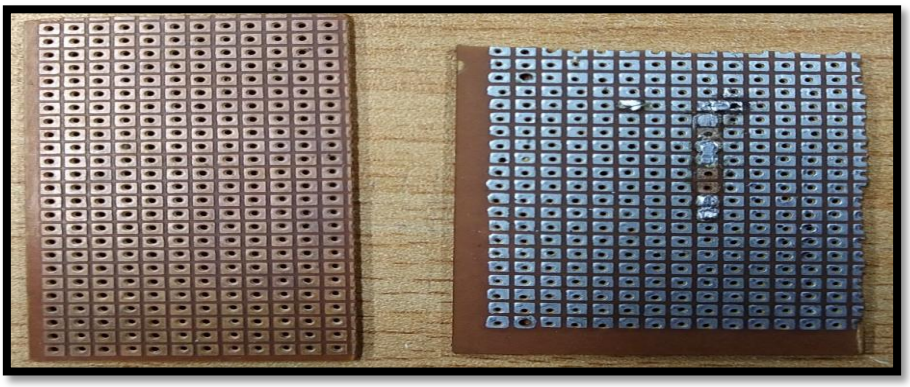


Fig 2.13 : Photographic view of V-Board

ii. Next the most important job is to create the circuit on bread board as shown in the fig 2.14. Basic bread board connections are relatively simple as we have used jumper wires for proper connections. But the problem of the connections on the bread board is that the connections are not that rigid and there is a problem of loose connections and accidentally pulling the wires from their required positions which can really hamper the effectiveness of the system. So there is an obvious need of finding a solution to that and we have moved towards the soldering of the circuit on v-board.

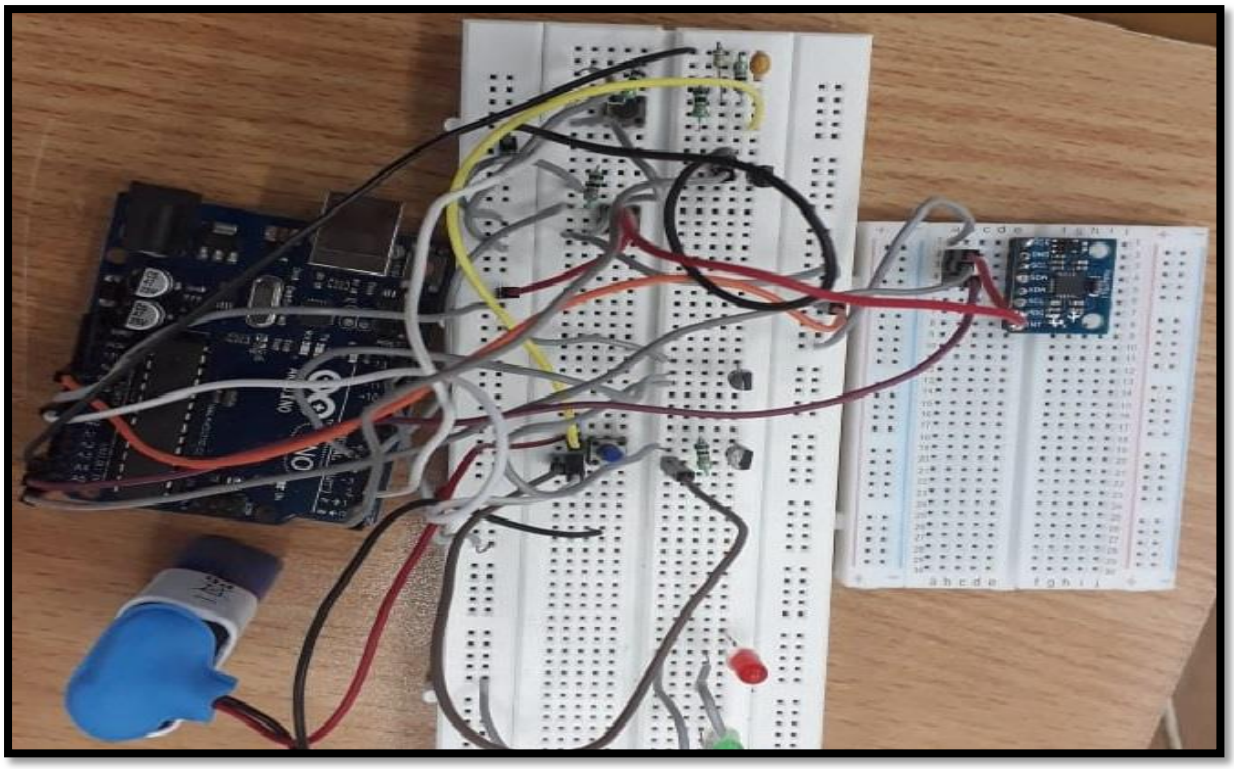
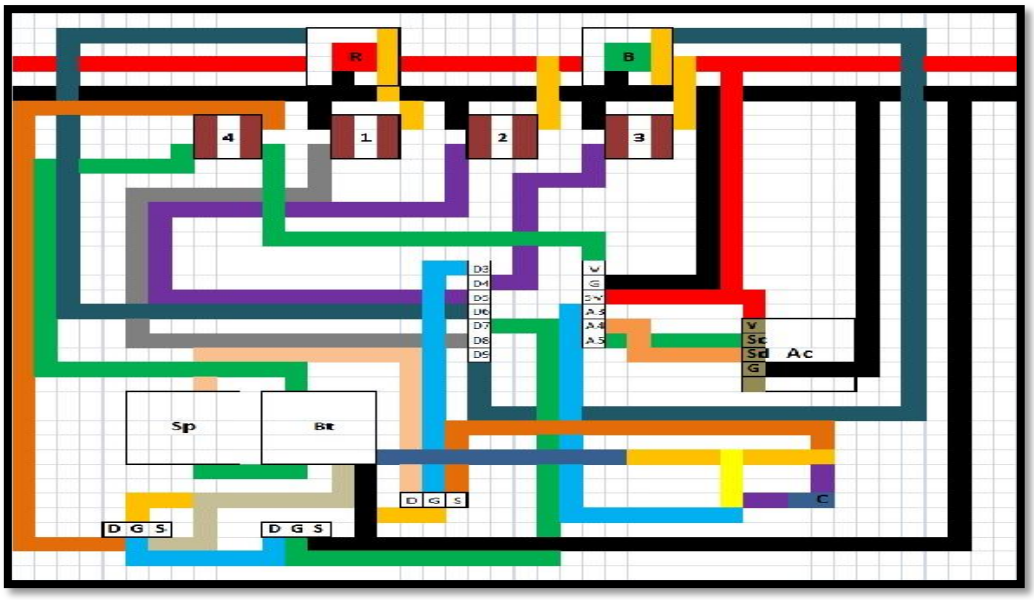


Fig 2.14 Photographic View of Circuit on Bread board

iii. Next job is to create the circuit on excel sheet to realize the space allocation on the v-board. That means to allocate individual components on it. One thing needed to be kept in mind that MPU6050 and arduino are not on the v-board so other components are needed to be allocating a proper space. In the fig 2.15 Red lines denotes 5V line and black line denotes ground terminal. Light yellow colour spaces are occupied by resistors and capacitor is denoted as ‘c’. 4 pin buttons are denoted by square blocks and red and green led’s are denoted as blocks with respective colours.



2.15: Space Allocation on Excel Sheet

iv. After the space allocation next job is to cut v-board in to a required piece in order to make the design shrink.

v. After that process we have to put all the components on the vero board following the excel sheet to manage the space. And simultaneously soldering all the components to their position. Connections are also made with the male and female jumper wires with the accelerometer and arduino.

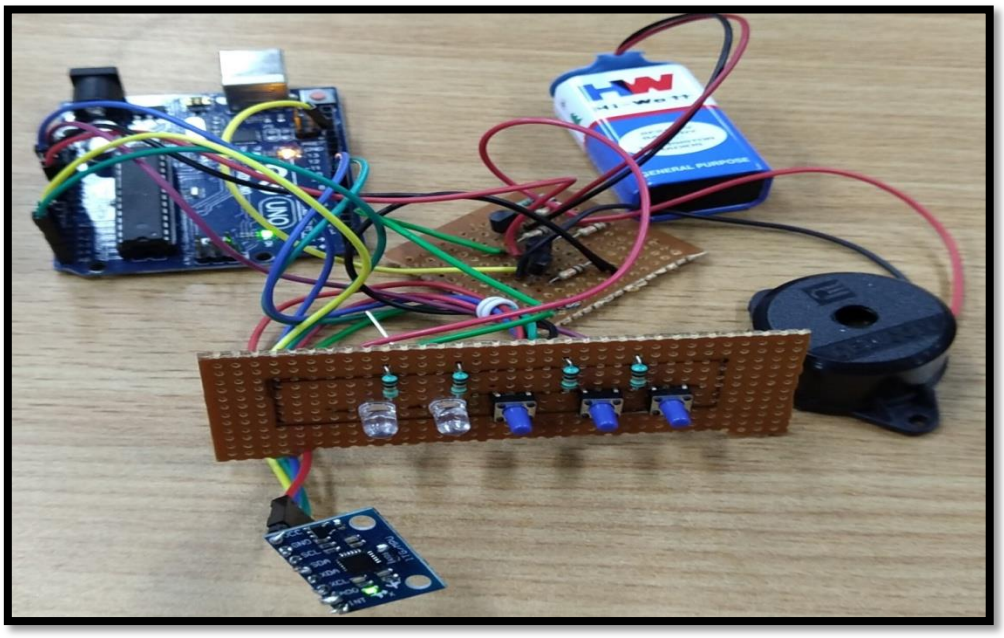


Fig 2.16: Photographic Image of Soldered components

d) **Uploading the programme on Arduino:** The Arduino development environment contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions, and a series of menus. Software written using Arduino is called sketches. It has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino environment including complete error messages and other information. Now let us install the Arduino into our system and start working with it.

Here are the steps that have been taken to upload the programme on Arduino board-

i. Step-1: Firstly Arduino IDE software is installed in our computer. This software is free and we can sketch anything on this software and later can upload it on Arduino. Arduino can hold only one programme at a time.

ii. Step-2 :When have open the Arduino IDE software there the work space will be looking like this-

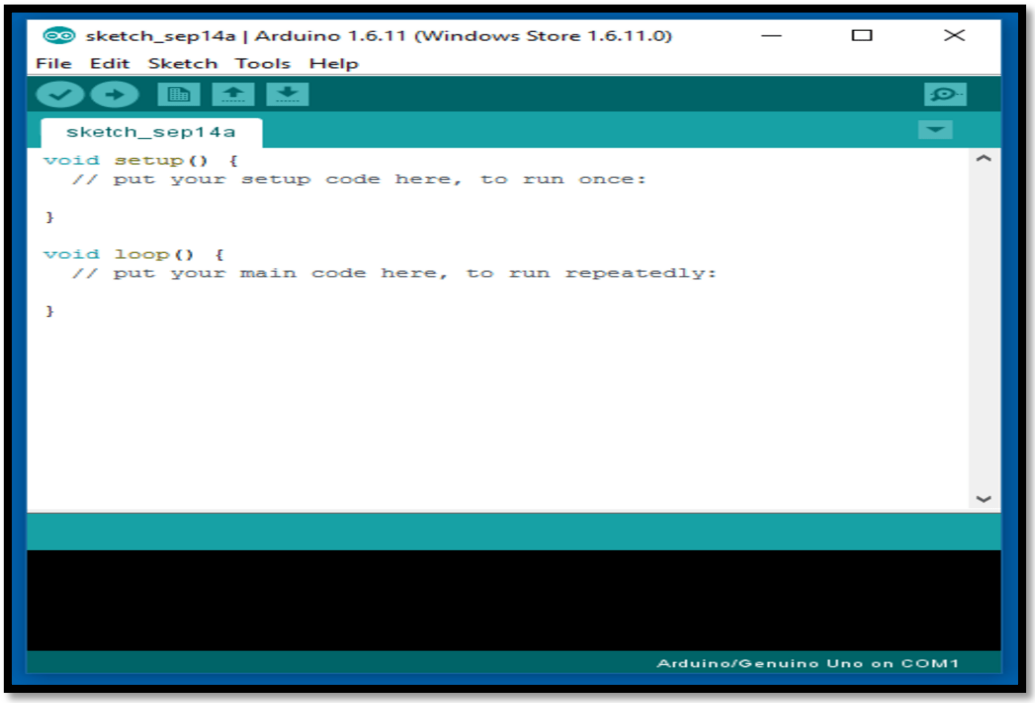


Fig 2.17: Photographic view Arduino UNO work space

iii. Step-3: At this moment we are pretty much familiar with the fact that what is needed to be done and then we plug in one end of the USB cable

to Arduino board and another to the Laptop. Then we have to tell Arduino IDE software that what is the board such as it is a Arduino UNO board. The complete procedures are discussed in following points.

iv. Step-4: Now we have to select port with which Arduino UNO board is attached as shown in the fig 2.18-

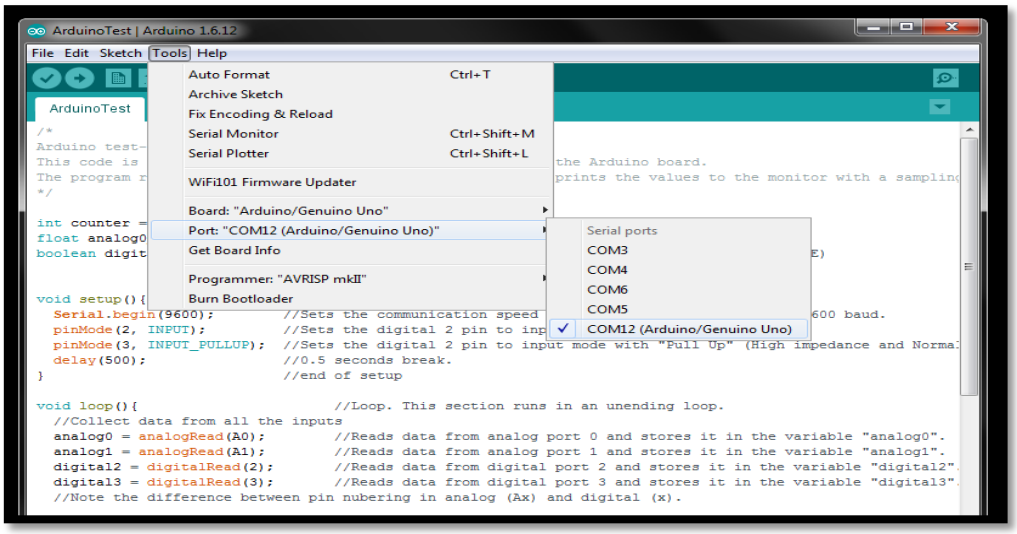


Fig 2.18: Photographic Image of Port Selection

v. Step-5: Then we have uploaded the programme and after compilation we have uploaded it on UNO board-

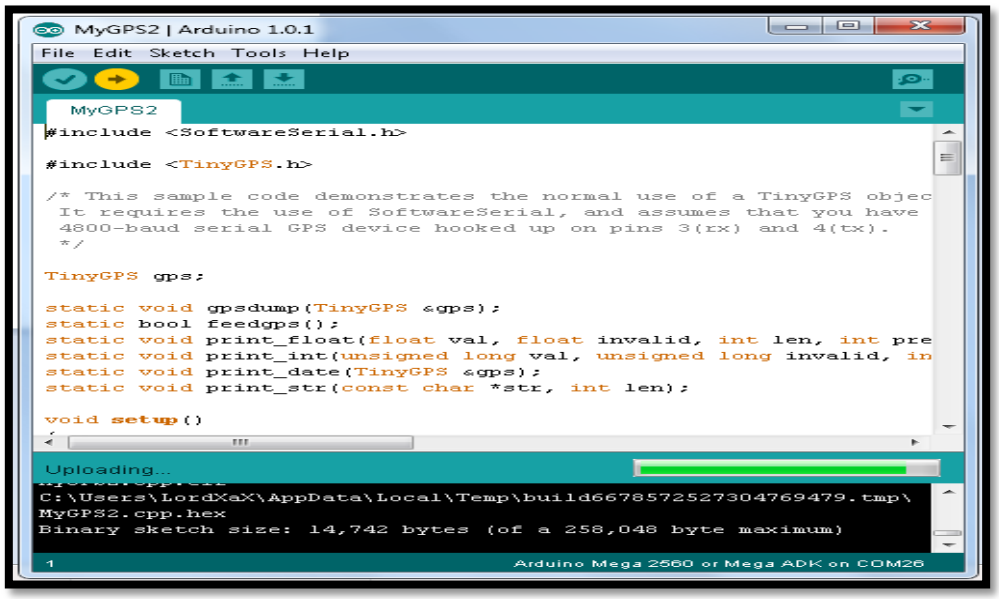
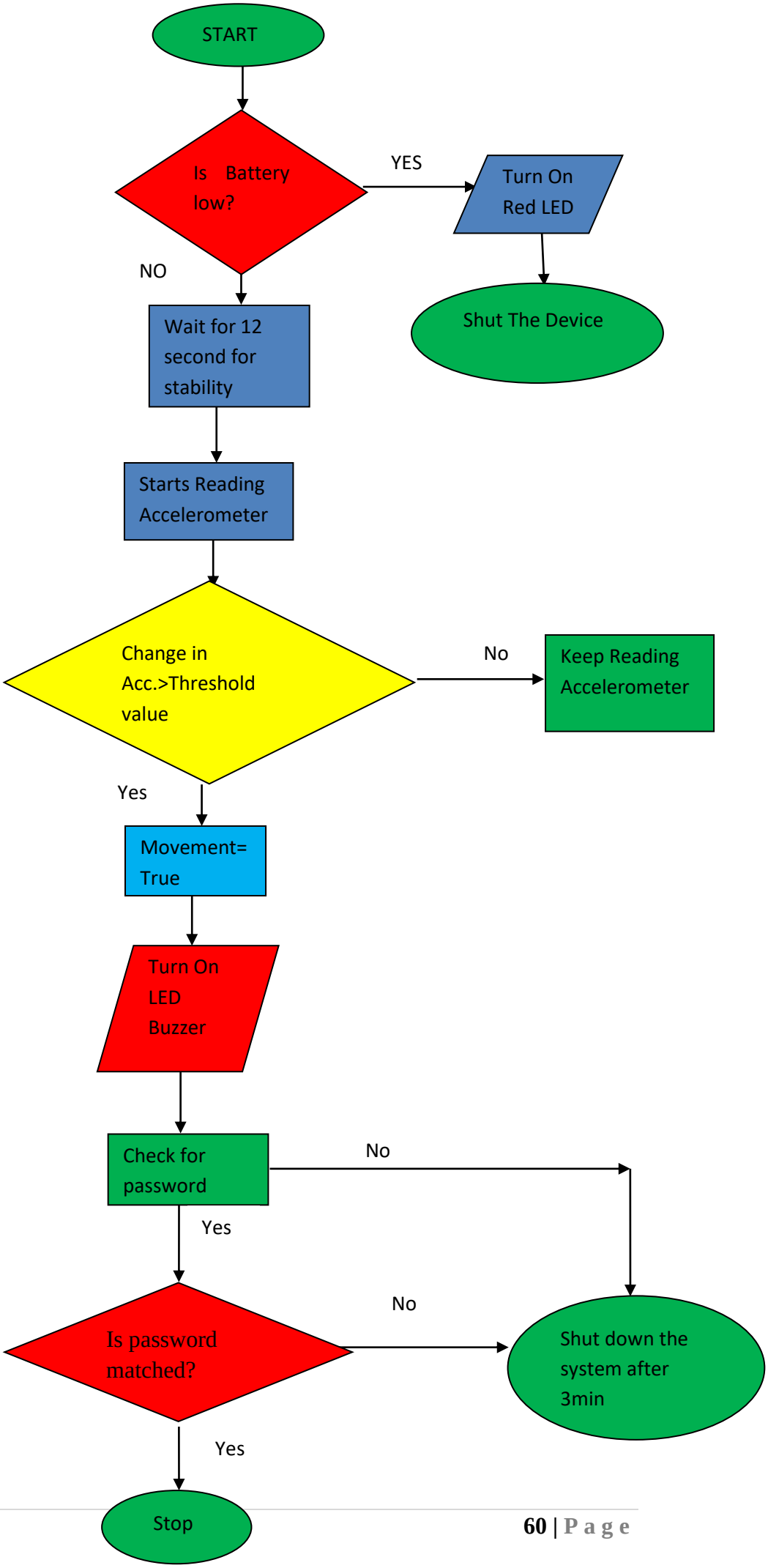


Fig 2.19: Photographic Image of Uploading on Arduino

e) **Serial communication:** Used for communication between the Arduino and a computer or other devices. All Arduino boards have at least one serial port (also known as a UART or USART): Serial. It communicates on digital pins 0 (RX) and 1 (TX) as well as with the computer via USB. Thus, if one use these functions, one cannot also use pins 0 and 1 for digital input or output. One can use the Arduino environment's built-in serial monitor to communicate with an Arduino board. Click the serial monitor button in the toolbar and select the same baud rate used in the call to begin(). Information passes between the computer and Arduino through USB cable. Information is transmitted as 0's and 1's, also known as bits.

   i. Compiling turns your program into binary data (ones and zeros)
   ii. Uploading sends the bits through USB cable to the Arduino
   iii. The two LEDs near the USB connector blink when data is transmitted
   iv. RX blinks when the Arduino is receiving data
   v. TX blinks when the Arduino is transmitting data

f) **Programme flow chart:** In the next page flow chart of the programme is given-


START
Is Battery low?
YES
Turn On Red LED
Shut The Device
NO
Wait for 12 second for stability
Starts Reading Accelerometer
Change in Acc.>Threshold value
No
Keep Reading Accelerometer
Yes
Movement= True
Turn On LED Buzzer
Check for password
No
Yes
Is password matched?
No
Shut down the system after 3min
Yes
Stop

g) Microcontroller Programming: There are several important parts of the programme that has been used to implement the anti-theft alarm system. Only the important parts which can be varied by the user is discussed below-

1) In the programming there is a provision of manipulating the secret code given by the user. Here in our project long pressing and short pressing of password buttons is used to turn off the system after the theft is detected by the owner. Here in this system PW1 has been considered for long press and PW2 has been considered as the short press. PW1 button is pressed and hold for "2000 to 6000" milliseconds and PW2 is pressed and hold for "50 to 1500" milliseconds. Below portion of the programme is given where the secret code is explained-

```
"if(readingA == HIGH && oldread == LOW){

currentmillisforcA = millis();

oldread = readingA;

}

if(readingA == LOW && oldread == HIGH){

currentmillisforcA2 = millis();

oldread = readingA;

if((currentmillisforcA2-currentmillisforcA) >=2000 && (currentmillisforcA2-
currentmillisforcA) <=6000){

cA = true;

}
```

```
else{

cA = false;

oldread = readingA;

}

}

else{

isMatched = false;

}

}

if(cA == true && cB == false){

byte readingB= digitalRead(pushbutton2);

isMatched = false;

if(readingB == HIGH && oldreadA == LOW){

currentmillisforcB = millis();

oldreadA = readingB;

}

if(readingB == LOW && oldreadA == HIGH){

currentmillisforcB2 = millis();

oldreadA = readingB;

if((currentmillisforcB2-currentmillisforcB) >= 50 && (currentmillisforcB2-
currentmillisforcB)<=1500){
```

```
cB = true;
}
else{
cA = false;
cB = false;
oldreadA = readingB;
}
}
else{
isMatched = false;
}
}
if(cA == true && cB == true){
isMatched = true;
}
else{
isMatched = false;
}
if(isMatched == true){
shuttdown();
```

}”

2) There is also some provision on selecting a proper sensitivity of the accelerometer used such that small movements do not trigger the alarm. And also 20% threshold limit is considered above which things are considered moving. Part of the programme is given below where accelerometer sensitivity is considerd-

“int AcSensitivity = 500;

const int maxMovementTime = 5000;

const int maxStillnessThreshold = 20;

const int readMPUinterval = 250;

const int settletime=5000;”

3) Also there is a provisions of selecting a proper tone sound for ease of detection of theft or burgling. This tune can be changed through programme as shown below-

“VoidspeakerPlayPiezo(booleanisSpeakerOn){ .

if (isSpeakerOn == true) {

tone(speakerpin, 200, 1000);.

} //end if isSpeakerOn

} //end speakerPlayPiezo”

Chapter 3

Design and Development of Project Box

The circuit design and development of anti-theft alarm system. Now we are planning to do make that system a commercially friendly. For that purpose we have planned to integral that system into a 3D printed project box which is light weight, beautiful and most importantly fully customized according to the need of the operator. We have also given our thought towards the economic side of making a project box which should not give a thought to the user about installing the anti-theft alarm system. So our main focus in this chapter will be knowing the basics of 3DP process and implementing that towards making a well customized project box.

3.1 Additive manufacturing:

Additive Manufacturing (AM) is an appropriate name to describe the technologies that build 3D objects by adding layer-upon-layer of material, whether the material is plastic, metal, concrete or one day human tissue. Common to AM technologies is the use of a computer, 3D modelling software (Computer Aided Design or CAD), machine equipment and layering material. Once a CAD sketch is produced, the AM equipment reads in data from the CAD file and lays downs or adds successive layers of liquid, powder, sheet material or other, in a layer-upon-layer fashion to fabricate a 3D object. The term encompasses many technologies including subsets like 3D Printing, Rapid Prototyping (RP), Direct Digital Manufacturing (DDM), layered manufacturing and additive fabrication. AM application is limitless. Early use of AM in the form of Rapid Prototyping focused on preproduction visualization models. More recently, AM is being used to fabricate end-use products in aircraft, dental restorations, medical implants, automobiles, and even fashion products.

In the next page we have shown the basic concepts of additive manufacturing.

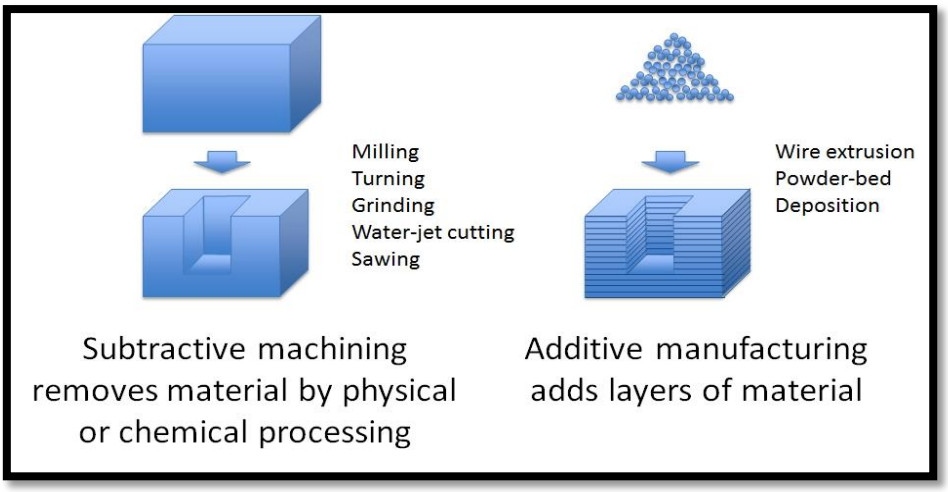


Fig 3.1 :Concepts of Additive Manufacturing

3.2 Subtractive Manufacturing:

Although emergence of additive manufacturing approach is considered as third industrial revolution, traditional techniques including subtractive manufacturing and forming are still advantageously utilized in different fields of manufacturing. Subtractive manufacturing indicates all those processes where material is removed layer by layer from a solid block to obtain desired 3-D component. All CNC based conventional machining processes (like turning, milling, drilling, etc.), non-traditional machining processes (like CHM, EDM, LBM, etc.) as well as newly developed micro and precision machining processes (like micro-milling, diamond turning, etc.) follow subtractive manufacturing approach. Now-a-days these processes utilize computerized system (CNC control) inbuilt with design software (CAD) and integrated manufacturing facility (CAM and CAPP). Initially a CAD drawing is created for the required component and an optimum process plan is generated considering a number of operating parameters including raw material, machine capability, tool availability, level of quality and tolerance requirement, etc. Based on this plan, programs are generated and it is fed to the machine. Machining is then carried out as per the program and excess material is removed in various ways (shearing, erosion, melting, sputtering, dissolution, etc.) in order to get desired object. In absence of CAPP, computerized process plan and automatic retrieval of part program is not feasible. In such cases, programs can be written manually.

3.3 Advantage and Disadvantage of Subtractive manufacturing:

There are several advantage and disadvantage of working in subtractive manufacturing and a detailed analysis has been conducted to compare additive and subtractive manufacturing.

There are lots of advantages of using a traditional method of manufacturing but important of those is discussed below

i. Wide variety of materials can be processed.
ii. Large size objects can be fabricated.
iii. Processes are faster.
iv. Subtractive manufacturing produces lower, more capable tolerances than additive manufacturing.
v. Subtractive methods result in smoother surfaces than additive methods. Additive manufacturing creates micro-pores, which can lead to infection in medical uses and also add fatigue points that can lead to stress fractures with heavy loads.
vi. Parts intended for long-term use or high-stress use are best made with subtractive manufacturing.
vii. Medical and aerospace industries prefer subtractive for parts required to stay in the body for long periods of time and for flight-critical aerospace functions.

Dis-advantages of Subtractive Manufacturing:

Cannot alter volumetric density of building material.

i. Material wastage takes place.
ii. Process planning is mandatory (it is laborious task that needs a lot of data).
iii. Limited capability in feature form (enclosed features cannot be generated).

3.4 Types of Additive manufacturing:

There are different types of additive manufacturing process. There is a growing interest of using additive manufacturing rather than subtractive manufacturing as it is versatile, it can also be atomized, variety of product development can be made with ease. Following are the different types of additive manufacturing that is nowadays in use-

i. **SLA**:

   Very high end technology utilizing laser technology to cure layer-upon-layer of photopolymer resin (polymer that changes properties when exposed to light).

The build occurs in a pool of resin. A laser beam, directed into the pool of resin, traces the cross-section pattern of the model for that particular layer and cures it. During the build cycle, the platform on which the build is repositioned, lowering by a single layer thickness. The process repeats until the build or model is completed and fascinating to watch. Specialized material may be needed to add support to some model features. Models can be machined and used as patterns for injection molding, thermoforming or other casting processes.

ii. **FDM:**

Process oriented involving use of thermoplastic (polymer that changes to a liquid upon the application of heat and solidifies to a solid when cooled) materials injected through indexing nozzles onto a platform. The nozzles trace the cross-section pattern for each particular layer with the thermoplastic material hardening prior to the application of the next layer. The process repeats until the build or model is completed and fascinating to watch. Specialized material may be need to add support to some model features. Similar to SLA, the models can be machined or used as patterns. Very easy-to-use and cool.

iii. **MJM**:

Multi-Jet Modelling is similar to an inkjet printer in that a head, capable of shuttling back and forth (3 dimensions-x, y, z)) incorporates hundreds of small jets to apply a layer of thermo polymer material, layer-by-layer.

iv. **3DP:**

This involves building a model in a container filled with powder of either starch or plaster based material. An inkjet printer head shuttles applies a small amount of binder to form a layer. Upon application of the binder, a new layer of powder is sweeped over the prior layer with the application of more binder. The process repeats until the model is complete. As the model is supported by loose powder there is no need for support. Additionally, this is the only process that builds in colors.

v. **SLS:**

Somewhat like SLA technology Selective Laser Sintering (SLS) utilizes a high powered laser to fuse small particles of plastic, metal, ceramic or glass. During the build cycle, the platform on which the build is repositioned, lowering by a single layer thickness. The process repeats until the build or model is completed. Unlike SLA

technology, support material is not needed as the build is supported by unsintered material.

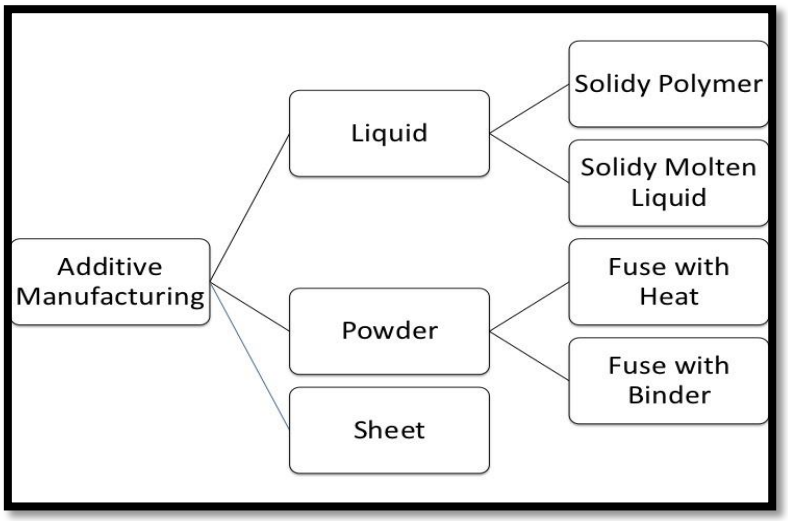


Fig 3.2: Varieties of Additive Manufacturing

3.5 Pros and Cons of Additive manufacturing:

a) **Advantages:**

i. Complexity is free: It actually costs less to print a complex part instead of a simple cube of the same size. The more complex (or, the less solid the object is), the faster and cheaper it can be made through additive manufacturing.

ii. Variety is free: If a part needs to be changed, the change can simply be made on the original CAD file, and the new product can be printed right away.

iii. No assembly required: Moving parts such as hinges and bicycle chains can be printed in metal directly into the product, which can significantly reduce the part numbers.

iv. Little lead time: Engineers can create a prototype with a 3-D printer immediately after finishing the part's stereo lithography (STL) file. As soon as the part has printed, engineers may then begin testing its properties instead of waiting weeks or months for a prototype or part to come in.

v. Little-skill manufacturing: While complicated parts with specific parameters and high-tech applications ought to be left to the professionals, even children in elementary school have created their own figures using 3-D printing processes.

vi. Few constraints: Anything you can dream up and design in the CAD software, you can create with additive manufacturing.

vii. Less waste: Because only the material that is needed is used, there is very little (if any) material wasted.

viii. Infinite shades of materials: Engineers can program parts to have specific colours in their CAD files, and printers can use materials of any colour to print them.

b) **Disadvantages:**

i. Slow build rates: Many printers lay down material at a speed of one to five cubic inches per hour. Depending on the part needed, other manufacturing processes may be significantly faster.

ii. High production costs: Sometimes, parts can be made faster using techniques other than additive manufacturing, so the extra time can lead to higher costs. Additionally, high-quality additive manufacturing machines can cost anywhere from $300,000 to $1.5 million, and materials can cost $100 to $150 per pound.

iii. Considerable effort in application design and setting process parameters: Extensive knowledge of material design and the additive manufacturing machine itself is required to make quality parts.

iv. Requires post-processing: The surface finish and dimensional accuracy may be lower quality than other manufacturing methods.

v. Discontinuous production process: Parts can only be printed one at a time, preventing economics of scale.

vi. Limited component size/small build volume: In most cases, polymer products are about 1 cubic yard in size, while metal parts may only be one cubic foot. While larger machines are available, they will come at a cost.

vii. Poor mechanical properties: Layering and multiple interfaces can cause defects in the product.

3.6 Concepts of 3D printing:

The term 3D printing covers a variety of processes in which material is joined or solidified under computer control to create a three-dimensional object, with material being added together (such as liquid molecules or powder grains being fused together), typically layer by layer. In the 1990s, 3D printing techniques were considered suitable only for the production of functional or aesthetical prototypes and a more appropriate term was rapid prototyping. Today, the precision, repeatability and material range have increased to the point that some 3D printing processes are considered viable as an industrial production technology, whereby the term additive manufacturing can be used synonymously with 3D printing. One of the key

advantages of 3D printing is the ability to produce very complex shapes or geometries, and a prerequisite for producing any 3D printed part is a digital 3D model or a CAD file. The most commonly used 3D Printing process is a material extrusion technique called fused deposition modelling (FDM). Metal Powder bed fusion has been gaining prominence lately during the immense applications of metal parts in the 3D printing industry. In 3D Printing, a three-dimensional object is built from a computer-aided design (CAD) model, usually by successively adding material layer by layer, unlike the conventional machining process, where material is removed from a stock item, or the casting and forging processes which date to antiquity. The term "3D printing" originally referred to a process that deposits a binder material onto a powder bed with inkjet printer heads layer by layer. More recently, the term is being used in popular vernacular to encompass a wider variety of additive manufacturing techniques. United States and global technical standards use the official term additive manufacturing for this broader sense.

3.6.1 Working Principles of FDM:

FDM is a process using molten plastics or wax extruded by a nozzle that traces the parts cross sectional geometry layer by layer. FDM creates tough parts that are ideal for functional usage. FDM works on an “additive” principle by laying down material in layers. A plastic filament or metal wire is unwound from a coil and supplies material to an extrusion nozzle which turns the flow on and off. The nozzle is heated to melt the material and can be moved in both horizontal and vertical directions by a numerically controlled mechanism which is directly controlled by a computer-aided design software package. The model or part is produced by extruding small beads of thermoplastic material to form layers as the material hardens immediately after extrusion from the nozzle plant.

a) Materials Used:

Many different materials can be used for 3D printing, such as ABS plastic, PLA, polyamide(nylon), glass filled polyamide, stereo lithography materials (epoxy resins), silver, titanium, steel, wax, photopolymers and polycarbonate.

b) Various Systems and mechanisms of FDM:

In order to create a complex physical object from a digital set of instructions, many mechanical systems must work together to get the job done correctly. In addition to these

mechanical systems, software used to control the nozzle temperature, motor speeds & direction, and methods in which the printer lays out the material are equally important to create a highly accurate model. This section will describe these various systems and how they contribute to the overall operation of the 3Dprinter.

The nozzle in a 3D printer has one of the most important jobs of all the mechanical systems. It is the last mechanical device that is used to build up a 3D object and its design and functionality is extremely important when it comes to the accuracy and build quality of the printer. The biggest contributor to the performance of the nozzle is its orifice size. Typically, the nozzle size used on many 3D printers is 0.4mm. This size is small enough to produce high quality parts while maintaining reasonable build times. Printers such as the Makerbot Replicator use this size nozzle. Depending on the over-all goal of the part being printed however , these nozzles can be changed to larger diameters in order to increase the speed of the print job. While doing so will decrease the horizontal accuracy, parts that will be use rough drafts or that will be post processed with fillers or paints will still perform as in-tended. It is important to never set the layer height higher than the nozzle size. This will dramatically decrease the bond strength between the layers and overall build quality. For example, if a 3D printer is using a 0.6mm nozzle, then the maximum layer height should not exceed0.5mm.While the nozzle is used to direct molten plastics in a precise manner, it's other job is to convert the solid coil of plastic material into the molten state by utilizing a heating element within the extruder assembly. This heating element can be a vitreous enamel resistor, a nichrome wire, or a cartridge heater. In addition to the heating element, there is usually a thermistor (temperature sensor) integrated into the extruder assembly to control the required temperature for the specific material being used. For example, one of the most common materials used in FDM is PLA(poly lactic acid) which has a melting temperature of around 160 degrees Celsius. In contrast, another very popular material used is nylon. This material requires extrusion between 240 and 270 degrees Celsius. It is very important to use the correct extrusion temperature in order to minimize the risk of the nozzle jamming and also maximize the bond between bead layers. The design of the extruder is very important to not only the printing accuracy, but also to the overall performance and maintenance of the printer. While the bottom end of the extruder must be able to heat the material to a desired temperature within a few degrees, the upper end must remain as cool as possible in order to avoid jamming. This is due to the feed mechanism located above the extruder, which requires the filament material to be in a completely solid state in order to function properly. One way

to decrease heat transfer from the heating element to the feed mechanism and in turn decreasing the chance of jamming is to use fans to cool the top end of the extruder. Depending on the type of model being printed, and the type of material being used, a heated bed may be important to maintain the structure's shape while it cools. Since plastics shrink as they cool, a quick temperature drop could cause the corners of a part to curl up off of the printer bed. To minimize this risk, some printers incorporate an electronically heated bed that keeps the temperature steady. This allows the model to cool at a more even rate and improve its overall dimensional accuracy. There are many factors that contribute to the build quality of a 3D printed part. As mentioned previously, the extruder assembly which includes the extruder, heating element, & nozzle contribute greatly to the overall build quality. In this section, additional factors that contribute to build quality will be discussed.

c) Filament:

When a conventional FDM printer is broken down, it is surprising to see how basic the technology really is. In its most basic form, the FDM printer is just a hot glue gun that is controlled with XYZ motors. In order to create accurate models however, these components must be able to work together under the assumption that the filament flow rate is constantly known. While the printer can easily estimate the flow rate based on the extruder speed and known nozzle diameter, it must also rely on the quality of the filament being used.

Depending on the software being used to print an object, the user can utilize a wide range of different to modify the method in which the model is printed. Some of these additional features are:

i. **Layer Height:**

This is the vertical height change from one layer to the next. While a smaller layer height yields a higher resolution part, the build time is much longer. On the other hand, large layer heights take much less time to produce but also decrease the surface quality. As mentioned before, the layer height must not exceed the nozzle diameter. This will lead to little or no bond between the layers.

ii. Perimeters:

This is the number of times the printer will draw the outer surface of a layer before proceeding on to the infill. Usually, there are 2 layers printed before the infill is done. The user may select to add more layers in order to increase the strength of the outer surface. This will however, increase the build time.

iii. Solid Layers:

This option allows you to specify the number of bottom and top layers. Usually it is advised to use 3 layers for the top and/or bottom surfaces. A setting of zero for the top layer will produce an outer shell type object much like a vase or pot.

iv. Fill Density:

This percentage number determines the amount of plastic in-fill there will be in an object. For example, a setting of 0.35 will fill 35% of the inner structures volume plastic material. Usually a setting of around 0.30 is used.

v. Generate Support Material :

It is common for more advanced software to allow the user to modify how the support material is utilized. Usually, this task is handled by the software automatically. There are certain cases where this may be beneficial. For example, if a user finds that a printed object is warped after it is completed, then adding additional supports to the object during the print process can help prevent this. Another example would mostly be used as a last resort. If the user finds that the bed of the printer is not level, then the Raft option could be used. This function builds a level layer of support material on the bed in order to create a level surface for the object to be printed on. Support structures which can be utilized properly are 'Touching build plate' which will be very helpful if bed is properly aligned and another one is 'support everywhere' which will be helpful if there is some overhanging part in the design.

vi. Speed:

The maximum speed of the machine is governed by the firm-ware installed on the motor controllers. However, it can be beneficial to adjust the speed in order to decrease the build time (fast) or increase the build quality (slow). The speed settings can be split in three categories; the perimeter, infill, and travel speed. The perimeter speed is the speed at which the print head moves while printing the perimeter of the mod-el. The infill speed is the speed at which the print head moves during the infill operation. And lastly, the travel speed is the speed at

which the print head moves from one location to an-other while not printing. For example, if there are multiple parts being printed at once, then the travel speed will be the speed of the print head when it is traveling to the other part to be printed. Typical speeds for the perimeter and infill are 50mm/sec and 70mm/sec, respectively.

vii. Brim Width:

The Brim Option is used to help large object being printed stick to the printer bed. Sometimes, large object will want to curl up at the corners due to warping. This option will print a horizontal ring around the first layer perimeter in order to increase the amount of material on the bed. This added bond strength will help prevent the part from warping.

viii. Sequential Printing:

While most 3D printing software can handle more than one object being printed at a time, sequential printing is a little different. The problem with printing multiple parts at once is that if one of the parts fails to print properly, then all of the other parts must be discarded as well. Sequential printing still prints multiple parts on the bed, however the parts are printed one at a time. This allows the printer to successfully complete part A before moving on to part B. Since the extruder has the potential of crashing in to the already printed parts, the user must specify a clearance distance in order to avoid any interference. While this process does take longer, it will save the user from having to discard a whole bed of parts in the case of an error.

ix. **Finishing:**

Though the printer-produced resolution is sufficient for many applications, greater accuracy can be achieved by printing a slightly oversized version of the desired object in standard resolution and then removing material using a higher-resolution subtractive process. The layered structure of all Additive Manufacturing processes leads inevitably to a strain-stepping effect on part surfaces which are curved or tilted in respect to the building platform. The effects strongly depend on the orientation of a part surface inside the building process. Some printable polymers such as ABS, allow the surface finish to be smoothed and improved using chemical vapour processes based on acetone or similar

solvents. Some additive manufacturing techniques are capable of using multiple materials in the course of constructing parts. These techniques are able to print in multiple colours and colour combinations simultaneously, and would not necessarily require painting. Some printing techniques require internal supports to be built for overhanging features during construction. These supports must be mechanically removed or dissolved upon completion of the print. All of the commercialized metal 3D printers involve cutting the metal component off the metal substrate after deposition. A new process for the GMAW 3D printing allows for substrate surface modifications to remove aluminium or steel.

x. **Multi Material Printing:**

Multi-material printing allows objects to be composed of complex and heterogeneous arrangements of materials. It requires a material being directly specified for each voxel inside the object volume. The process is fraught with difficulties, due to the isolated and monolithic algorithms. There are many different ways to solve these problems, such as building a Spec2 Fab translator. Or use microstructures to Control Elasticity in 3D Printing. There is also a solution about how to print a Multi-material 3d painting: Deep Multispectral Painting Reproduction via Multi-Layer, Custom-Ink Printing. Multi-material 3D printing is a fundamental element for development of future technology. It has been already applied to variable industries. Other than common applications in small manufacturing industries, to produce toys, shoes, furniture, phone cases, instruments or even art works. With the BAAM (Big Area Additive Manufacturing) machine, large products such as 3D printed houses or cars are quite feasible. It has also been widely used in high-tech industries. Researchers are devoting to producing high-temperature tools with BAAM for aerospace applications. In medical industry, a concept of 3D printed pills and vaccines has been recently brought up. With this new concept, multiple medications are capable of being united together, which accordingly will decrease many risks. With more and more applications of multi-material 3D printing, the costs of daily life and high technology development will become irreversibly lower. Metallographic materials of 3D printing are also being researched. By classifying each material, CIMP-3D can systematically perform 3D printing with multi materials.

3.7 Applications of 3D printing:

There are several applications of 3D printing and they are discussed below field wise-

a) Manufacturing Applications:
1) Cloud based additive manufacturing.
2) Mass customization.
3) Rapid prototyping.
4) Research application.
5) Food processing and Agile Tooling.

b) Medical Application:
1) Bio-Printing.
2) Medical devices and pills.

c) Industrial Application:
1) Apparel of different materials.
2) Industrial art and jewellery.
3) Automotive Industry.
4) Construction field.
5) Fire arms, computer and robots.
6) Space application

d) Socio cultural application:
1) Art and jewellery applications
2) 3D selfies communication purpose
3) Education and research

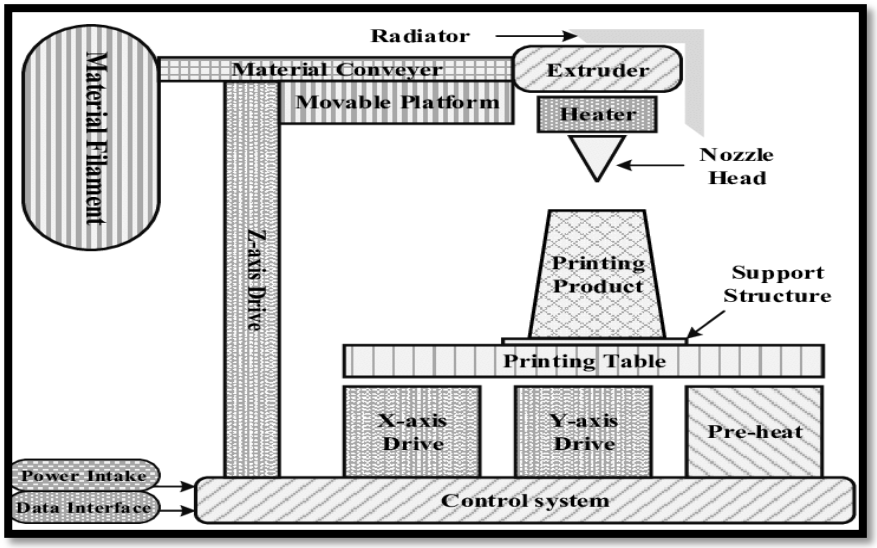


Fig 3.3: Basic operational principles of 3DP

3.8 Design and development of alarm box:

Finally the design of the 3D printed project box is started by properly analysing the related process parameters. Step by step the procedures of making a product in 3D printing is describes below-

i. First of all we have to draw project box according to the placement of several components in Autodesk fusion 360. Below we have shown photographic view of the screen of fusion 360-

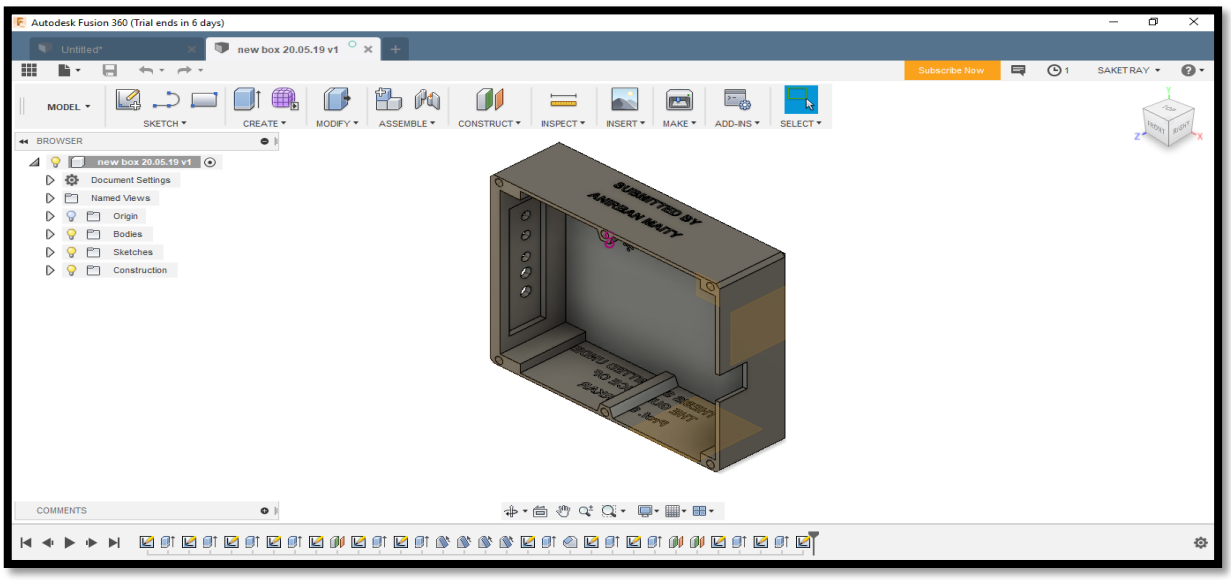


Fig 3.4 Designing of Project Box

ii. Then the box designed will be saved in .stl file

iii. Then the .stl file will be uploaded in Cura for slicing. In Cura we can actually see the way layer by layer the box can be produced

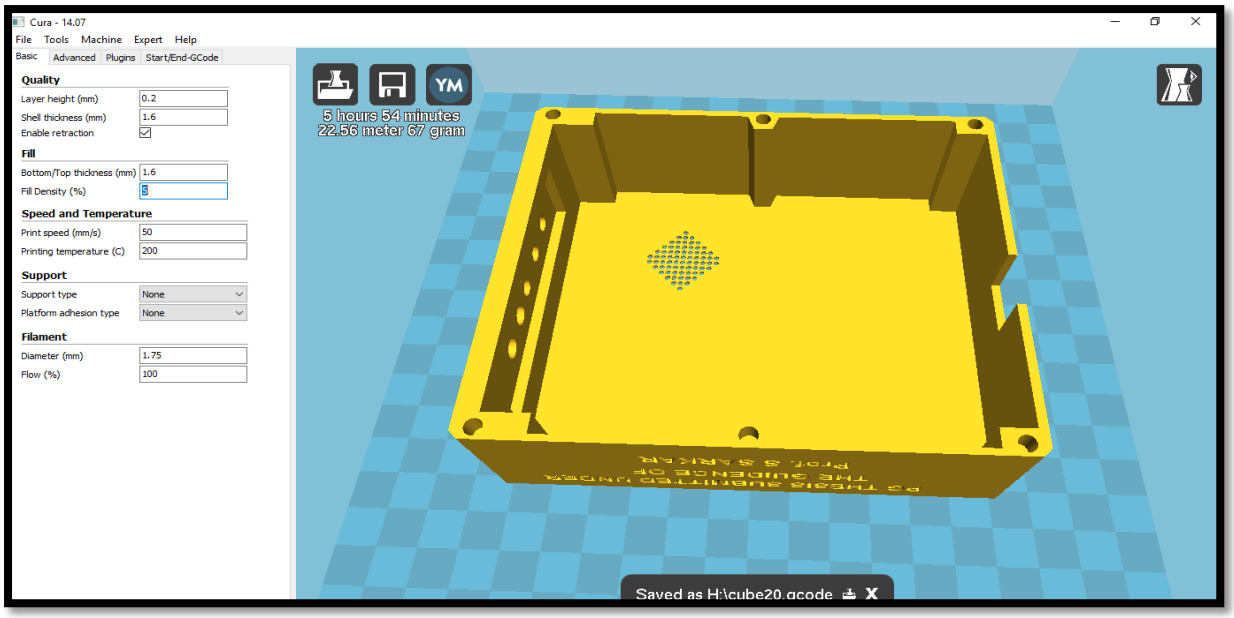


Fig 3.5 Box After being uploaded in cura

iv. Then the product is saved in terms of G-code file which can be read by FDM printer for 3D printing.

Then this G-code file with the help of card reader is uploaded in FDM printer for 3D printing. And after performing required commands 3D printing is started which is shown below-

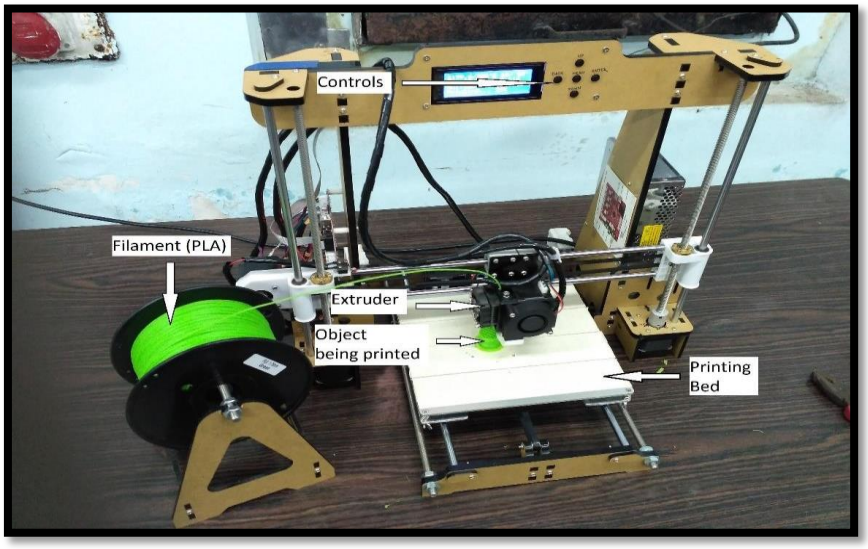


Fig 3.6: 3D Printer

3.9 Specifications of FDM machine:

Specifications of FDM machines includes the following important factors-

i. Layer Height: 0.2 mm

ii. Fill Density: 20%

iii. Print Speed: 30

iv. Extruder temperature: 200°C

v. Bed temperature: 60 °C

3.10 Assembling the various components inside the project box:

The product produced after successfully conducting 3DP is shown below. And the problems arises from the assembly designs are also discussed below-

i. Thickness of the box is taken as almost 2mm. Which has enough strength to incorporate better box?

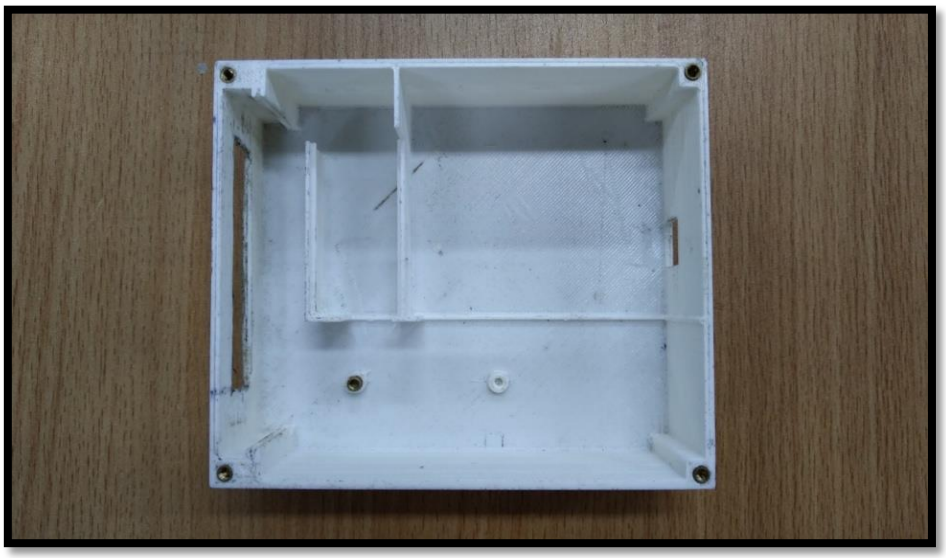


Fig 3.7: Photographic Image of Box obtained

ii. Letters are drawn on the box for better customization of the product.

iii. Then copper inserts have been installed in required hole for easy fastenings of our project box.

iv. For assembly purpose, properly fit all the components in a proper way. Several front covers have been made to see the proper positions of the buttons. And

every faulty design with their short comings are discussed below.

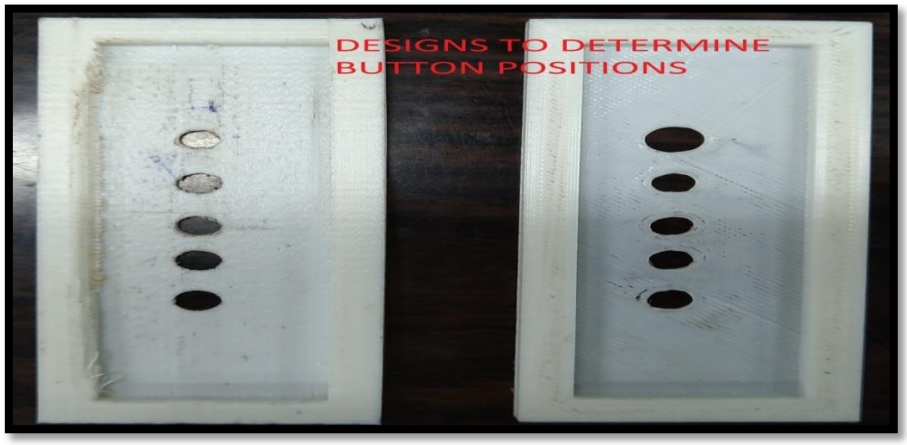


Fig 3.8 : Photographic view of covers

v. Finally a proper front cover has been made to accommodate our alarm system's buttons and LED. And the proper front cover is shown below.

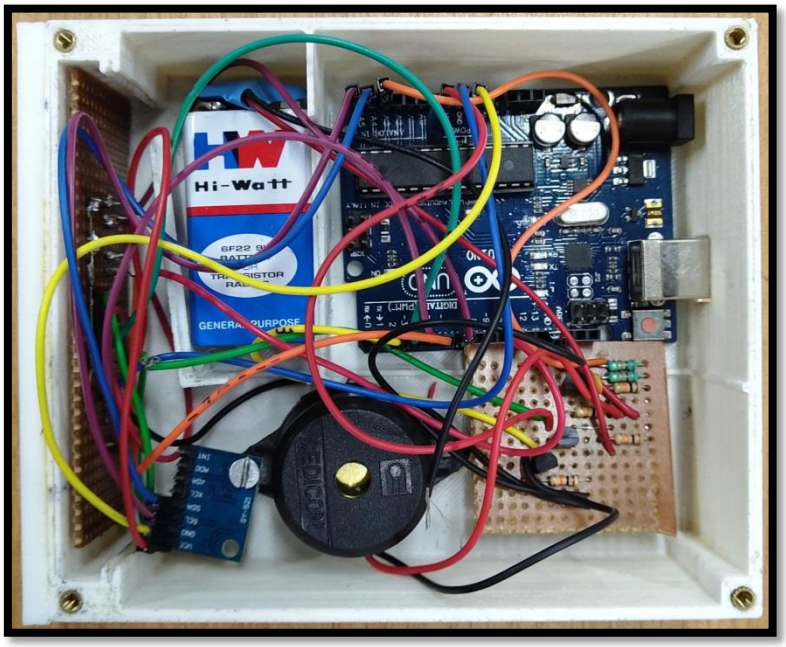


Fig 3.9: Photographic view of circuit inside the box

vi. Hole is incorporated into the box in order to change or customise the Arduino program.

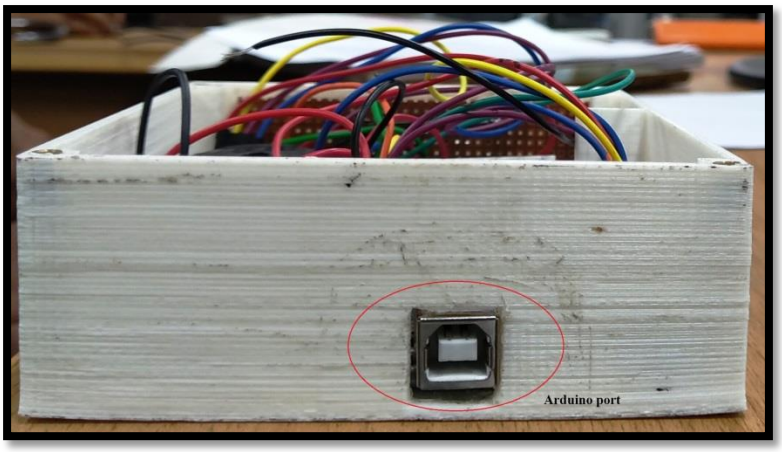


Fig 3.10: Photographic view of Arduino port

vii. Finally all the components are assembled into the box and then the proposed alarm box is installed in the bicycle.

Fig 3.11 Photographic view of alarm box

Fig 3.12 Photographic view of the alarm box installed on bicycle

Chapter 4

General Summary and Conclusions

In the present research study an attempt has been made to develop an anti-theft alarm system for bi-cycles. The objective here is to develop an anti-theft alarm system which can be attached to the bi-cycle. The anti-theft alarm system is intended to design in such a manner that if significant movement is detected (in armed/on condition), it will immediately trigger a sound for a certain period of time. For developing the alarm system following procedure has been adopted:

i. Initially various sensors were considered and finally MPU 6050 has been used and integrated with microcontroller considering its advantages over other sensors.
ii. A proper software programme with all the necessary functionalities has been developed.
iii. The circuit has been implemented on bread board and subsequently the circuit is soldered on vero board.
iv. Project box was designed by considering physical dimensions of the all components like vero board, Arduino UNO, Buzzer, and Battery using Auto Desk Fusion 360 CAD software. A careful attention was also given on proper positioning of the front buttons and LED's for ease of operations.
v. The designed project box was manufactured using 3D printer.
vi. All components were assembled to develop the alarm box.
vii. Finally the performance of the alarm box was tested and found quiet satisfactory for practical requirements.

The design covers all the vital areas of an alarm based anti-theft security device for bi-cycle and is quite cheap and its portability is also good enough for user. Nevertheless, the same anti-theft alarm system can be used for other purposes directly or with slight modification.

Still there is a possibility of future improvement of this alarm box. The future research scope of improving the alarm system is as follows:

i. Implementation of sensitivity adjustment facility by the user i.e. user can adjust the sensitivity of the alarm system as per their requirements.
ii. As it is a battery operated system further requirements on power consumption by optimizing the programme and selection of appropriate hardware (Microcontroller, MOSFET etc) configuration.
iii. There is also some scope of adding other sensors like vibration or shock sensors, Infra sound sensors, Ultrasonic sensors, photoelectric beam sensors etc. and study their usefulness in anti-theft alarm systems.
iv. There is also possibility of improvements by installing a GSM module to send SMS to user mobile for enhanced security, and also there can be some provision of sending emails through some module will be a step forward in IoT implementation.

BIBLIOGRAPHY

1. Holt, D., and Young, R. A. "The effect of intruder alarms on business losses, police activity and criminal behaviour in the United Kingdom". In Proceedings The Institute of Electrical and Electronics Engineers. International Carnahan Conference on Security Technology, pp. 461-464,1995.
2. Pascoe, T., and Lawrence, G. "Are intruder alarm systems effective as crime prevention measures?". In 1996 30th Annual International Carnahan Conference on Security Technology (pp. 226-231). IEEE.(1996).
3. Adriano, D. B., and Budi, W. A. C. "Iot-based Integrated Home Security and Monitoring System". In Journal of Physics: Conference Series (Vol. 1140, No. 1, p. 012006). IOP Publishing. (2006).
4. Song, H., Zhu, S., and Cao, G. "Svats: A sensor-network-based vehicle anti-theft system". In IEEE INFOCOM 2008-The 27th Conference on Computer Communications (pp. 2128-2136). IEEE (2008).
5. Wang, X., Wang, Y., and Xie, J. "Multifunctional intelligent wireless alarm system". In 2008 3rd IEEE Conference on Industrial Electronics and Applications (pp. 268-271). IEEE.(2008).
6. Meucci, F., Pierucci, L., Del Re, E., Lastrucci, L., and Desii, P. "A real-time siren detector to improve safety of guide in traffic environment". In 2008 16th European Signal Processing Conference (pp. 1-5). IEEE.(2008).
7. Andrejaši˘.M., "Mems Accelerometer".Marec (2008).
8. Lili, W., and Tiejun, C. "Automobile anti-theft system design based on GSM". In 2009 International Conference on Advanced Computer Control (pp. 551-554). IEEE.(2009).
9. Bin-feng, Y., Qiong, W., and Xiao-kan, W. "Design and realization of multifunctional and intelligent protection instrument for electric bicycle". In 2010 3rd International Conference on Computer Science and Information Technology (Vol. 3, pp. 190-193). IEEE. (2010).
10. Li, H., Yang, H. T., and Li, X. L. "Design and application of new kind of electronic and mechanical antitheft lock using DSP". In 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (Vol. 4, pp. 263-266). IEEE.(2010).

11. Omprakash, k. “Wireless Home Security System With Mobile”. IJAET,Vol.II, Issue IV, pp.396-397,(2011).
12. Brooks, D. J. “Intruder alarm systems: Is the security industry installing and maintaining alarm systems in compliance to Australian Standard AS2201?”. Security Journal, 24(2), pp.101-117, (2011).
13. Hu, J. M., Li, J., and Li, G. H. “Automobile anti-theft system based on GSM and GPS module”. In 2012 Fifth International Conference on Intelligent Networks and Intelligent Systems (pp. 199-201). IEEE, (2012).
14. Zungeru, A. M., Kolo, J. G., and Olumide, I. “A Simple and Reliable Touch sensitive security System”. arXiv preprint arXiv:1210.5973,(2012).
15. Ibrahim, V. M., and Victor, A. A. “Microcontroller based anti-theft security system using GSM networks with text message as feedback”. International Journal of Engineering Research and Development, 2(10), pp.(18-22), (2012).
16. Chodon, P., Adhikari, D. M., Nepal, G. C., Biswa, R., & Gyeltshen, S. “Passive Infrared (PIR) Sensor Based Security System”. International Journal of Electrical, Electronics & Computer Systems, 14(2),(2013).
17. Zungeru, A. M. “An electronic digital combination lock: A precise and reliable security system”. arXiv preprint arXiv:1303.1734,(2013).
18. Bangali, J.,and Shaligram, A. “Design and Implementation of Security Systems for Smart Home based on GSM technology”. International Journal of Smart Home, 7(6), pp.(201-208), (2013).
19. Lee, J. V., Chuah, Y. D.,and Chai, C. T. “A multilevel home security system (mhss)”. International Journal of Smart Home, *7*(2), pp.(49-60), (2013).
20. Farjana, H. N., Chandrasekaran, S. C., Gita, B., Bhuvaneswarri, J., Chandrasekaran, S. C., Miranda, M. G.,and Ramachandran, S. S. no Authors Title Vol Issue. JCDR, 20(14/8784.5235), 2249782X,(2014).
21. Omorogiuwa, E., and Elechi, P. “GSM Based Intelligent Home Security System for Intrusion Detection”. International Journal of Engineering and Technology, 4(10), pp.(596-605), (2014).
22. Sulochana, B., Sarath, B. A.,and Babu, M. “Monitoring and detecting vehicle based on accelerometer and MEMS using GSM and GPS technologies”. Int. J. Comput. Sci. Trends Technol.(IJCST), 2(4), pp.(55-59), (2014).

23. Samuel, D. R.,and Ojongbede, H. A. “Microcontroller Based Security System with Intruder Position”. IOSR Journal of Electrical and Electronics Engineering, 9(1), pp.(01-08), (2014).
24. Huan, J., Liu, X., Zhu, Z.,and Zhu, X. “A Burglar Alarm System Based on ZigBee and GSM for Aquaculture”. Sensors & Transducers, 175(7), pp.(273),(2014).
25. Fang, H., Yan, G.,and Li, H. L. “Design of remote car anti-theft system based on ZigBee”. In Sixth International Conference on Electronics and Information Engineering (Vol. 9794, pp. 97940X). International Society for Optics and Photonics.(2015).
26. Choudhury, B., Choudhury, T. S., Pramanik, A., Arif, and W.,Mehedi, J. “Design and implementation of an SMS based home security system”. In 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-7). IEEE,(2015).
27. Mamun, K. A.,and Ashraf, Z. “Anti-theft vehicle security system with preventive action”. In 2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE) (pp. 1-6). IEEE,(2015).
28. Shah, D., Nair, R., Parikh, V., and Shah, V. “Accident alarm system using gsm, gps and accelerometer”. International Journal of Innovative Research in Computer and Communication Engineering, 3(4), pp.3506-3511(2015).
29. Kale, A. S., Deshmukh, A. V., Benodkar, M. V., Nage, P. K., and Fukate, S. P. “Design of Banking Security System Using Mems And Rfid Technology”,(2015).
30. Nwalozie, G. C., Aniedu, A. N., Nwokoye, C. S., and Abazuonu, I. E. “Enhancing Home Security Using SMS-based Intruder Detection System”. International Journal of Computer Science and Mobile Computing, 4, pp.(1177-1184),(2015).
31. Divya, G., Sabitha, A., Sudha, D. S., Spandana, K., Swapna, N., and Hepsiba, J. “Advanced vehicle security system with theft control and accident notification using gsm and gps module”. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 4(3), pp.(64-68),(2016).
32. Chitnis, S., Deshpande, N., and Shaligram, A. “An investigative study for smart home security”: Issues, challenges and countermeasures. Wirel. Sens. Netw, 8(04), pp.(61-68), (2016).
33. Hossain, M. M., Islam, M. S., Dipu, N. F., Islam, M. T., Fattah, S. A.,and Shahnaz, C. “Design of a low cost anti-theft sensor for motorcycle security device”. In 2017 IEEE

Region 10 Humanitarian Technology Conference (R10-HTC) pp. (778-783). IEEE,(2017).

34. Iyapo, K. O., Egbuwalo, S. A., Akinbobola, A. J., & Oni, O. T. Design and Implementation of Motion Detection Alarm and Security System.(2017).