# CHAPTER TWO

**LITERATURE REVIEW**

## 2.1 Introduction

In this research work, literatures were reviewed which serve as a guide towards achieving the set aim and objectives. This chapter comprises of the review of fundamental concepts and review of similar works which were relevant to this research work.

## 2.2 Review of Fundamental Concepts

This section provides a review of applicable fundamental conceptions of home security systems. It covers the rudiments of both the hardware and software requirement of the security system, the description of applicable concepts and the definitions of related terms.

## Alarm/Security System

An alarm/warning system is a set of unified devices used to guard property or lives by providing a response to a danger, such as thief intrusion or fire outbreak. The response of the system can be either warning the residents about the hazard or activating an action that will solve it, such as automatic fire suppression (Tomek, 2017).

The key components of a typical alarm system are:

1. Sensors
2. Control panel
3. Warning devices and a keypad.

The control panel is the vital element that communicates with all the elements in the system. The linkage with the control panel is either wired or wireless. The sensors detect a certain predefined activity that leads to an alarm situation, such as glass breakage or sudden increase of temperature, and informs the control panel. The notifying devices, such as bells, sirens and flashing lights can be triggered by the control panel and serve to warn the residents about an emergency (Tomek, 2017).

### 2.2.1 Sensors

Human beings possess some biological detectors like the eye- sensing light. We can detect warmth, tension/strain, light, flavour, and so forth. However, sensor devices help significantly to extend our sensitivity as well as the level of our normal ability to things such as magnetic fields (Poncette *et al.*, 2019). Sensors, Detectors and Transducersare synonymous.

Sensors are the devices that measure data from adjoining environment and provides an electrical signal in response to the measurand (Tyler *et al*., 2019). They allow detecting, evaluation, and documentation of physical fact that is otherwise challenging to measure by transforming the data into a more suitable signal. The value of the original physical parameter can be calculated from the proper characteristics of the electrical signal (amplitude, pulse-width, frequency, etc). Electrical outputs are very easy to use because there are well known processes (and often readily available off-the-shelf solutions) for filtering and acquiring electrical signals for real-time or continuous evaluation (Graham, 2000).

Sensors can be classified as "smart sensors or intelligent sensors" (Syed *et al.,* 2019).

A Smartdetectoris a blend of detecting element, a non-digital interface circuit, an Analog Digital Converter (ADC) and a bus interface in a single case. An intelligentsensoris a detector that has one or more intelligent roles such as self-assessment, self-recognition, self-authentication, self-adaptation (Syed et al., 2019).

An intelligent sensor can detect a condition, respond to the condition, and be able to manage its purposes because of motivation from external functions (outside environment). This shows that intelligent sensors have the architecture of advance learning, modification, and signal administering, all in one integrated circuit. Intelligent sensors require specialised hardware called signal conditioning circuitry to monitor and control it and other appliances.

Sensors implemented for this system include photoelectric smoke detector, passive infrared motion detector (PIR) and gas detector.

2.2.1.2 *Passive Infrared Motion Detector (PIR****)***

Radiation is basically a field in space which has attributes of velocity, power, and frequency (Alex et al., 2019). Radiation in the wavelength that the human eye can see is very restricted. This radiation is called visible light, it is usually described in terms of its properties, using three models:

1. Wave Model

Radiation acting as an oscillating electromagnetic field travelling through space at the speed of light brings about dispersion, refraction, and analogous effects. Great number of systems for assessing or illustrating light use the wave model (Alex et al., 2019).

1. Particle Model

Radiation can act like a stream of discrete particles of vitality. These particles known as photons. Most detector’s response and reasons for their interaction with matter are accounted for by the photon model (Alex et al., 2019).

1. Ray Model

Light traveling from light source though air, focal points, or other straightforward substances and experiences reflections at mirrors is completely described as rays. In the explanation of imaging by lenses, wave model is inconsequential (Alex et al., 2019).

Radiation of energy is continuous for all objects, in the form of electromagnetic waves due to thermal vibrations of molecules of the objects. Electromagnetic radiation is emitted by any object with absolute temperature above zero at some wavelength which is in direct proportion to the object’s temperature. Using a known relationship between wavelength and temperature called Wien’s displacement law, we can calculate the peak wavelength of the radiation emitted by an object, such as human body. The law is given by Equation 2.1 (Richard Olsen, 2007) as:

(2.1)

(2.2)

where:

is constant given as 0.2898µmº

T is temperature of object in

In Celsius the average human temperature is approximately 34°C about 307°K.; the peak wavelength was calculated to be

Thus, this indicates that human body radiation peaks between 9 to 10, which rests in the infrared (IR) portion of electromagnetic spectrum. As illustrated in Figure 2.1.

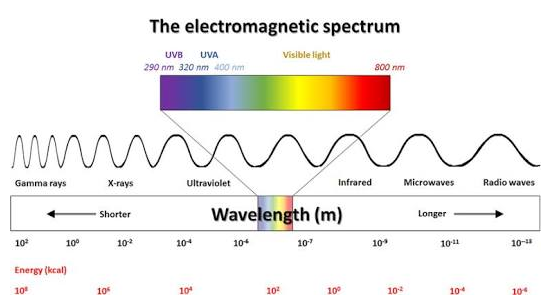


Figure 2.1: The Electromagnetic Spectrum (Giannakis *et al.,* 2016)

Passive Infrared Motion Detectors (PIRs) are also known as “Pyroelectric” or “IR Motion sensors” are of the most frequent detectors in households and miniature business environments. They are reasonably priced and gives consistent functionalities (David *et al.,* 2015). A PIR is a device that produces a surface electric charge when exposed to infrared radiation. The operation principle of PIR detector is to sense the change in temperature in its detection area (Luo and Chen, 2013). The sensor is divided into two halves to find not the radiation itself, but the variation in the situation that happens when a target enters its field. These variations in the quantity of infrared radiation on the element translate to changes in the voltage generated, measured by an on-board amplifier. High signal output from the PIR sensor is an indication of motion detection, which can be read by the microcontroller units.

A characteristic PIR has elements made of an electric charge generating crystalline material when visible to infrared energy. The crystalline material used in detecting element is susceptible to a broad scale of radiation. PIR detectors employed in motion sensors are mostly interested in the band within which the human body radiates; around 8 to 14, with peak wavelength of about 9.5the sensor package contains an infrared filter to limit the incoming radiation to human body range for this exact purpose. The sensor package has two sensing elements for motion detection, known as a dual-element sensor. The two sensing devices are connected in series position to achieve this. The voltages generated varies, depending on how much infrared energy strikes the element, which is monitored by an on-board amplifier. A Fresnel lens is used in the device to focus infrared signals onto the element. The on-board amplifier trips the output to indicate mobility as the ambient infrared signals vary rapidly. Figure 2.2 illustrates the working principle of a PIR.

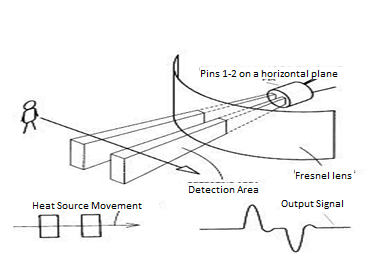


Figure 2.2 Focusing Device (kodali *et al.,* 2016).

Temperature and other environmental factors affect the PIR Sensor's sensitivity. Some PIR usually have onboard jumper which allows for selection of either normal operation or reduced sensitivity (Akinwumi *et al*., 2020). In general, when in decreased sensitivity mode, the PIR sensor will detect an item from up to half the distance it would in regular working mode.

Several factors affect the PIR Sensor’s range such as:

1. The jumper setting for sensitivity.
2. The size and thermal qualities of items in the immediate vicinity and
3. Environmental variables, such as temperature and light sources

Figure 2.3 presents a graph showing the effect of temperature on PIR distance detection.

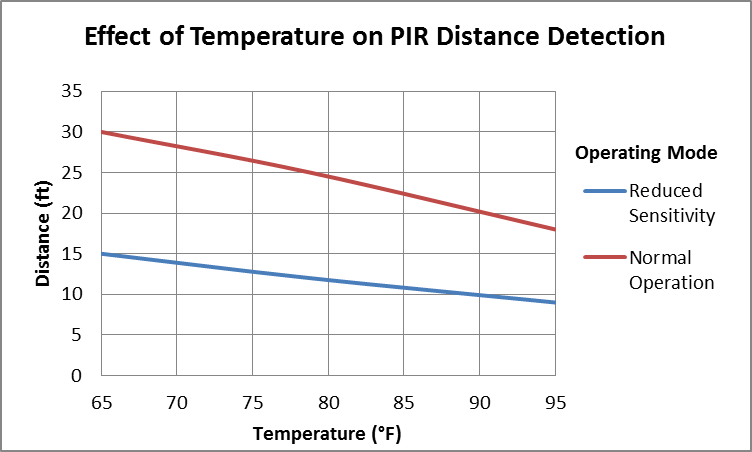


Figure 2.3: Temperature/Distance Relationship of a PIR (Pawar *et al.,* 2018)

It can be deduced that in both modes of operation, the temperature and distance of sensitivity/detection are inversely proportional, with an approximate ratio of 3:1.

A typical PIR has certain features that are standard defined, irrespective of its manufacturer.

(Akinwumi *et al.,* 2020), such as:

1. The ability to detect a person from about 10 meters, or up to 5 meters in decreased sensitivity mode.
2. Source current up to 12 mA at 3 V and 23 mA at 5 V
3. It is little enough to be hidden.
4. Contact to any microcontroller is simple.

2.2.1.3  *Gas Detectors*

A gas detector is a device that detects the presence of specific gases in a space, usually as part of a safety system. This technology is used to detect gas leaks and other types of pollution. When a toxic gas is discovered, a gas detector can sound an alarm to warn people. Combustible gas sensors, photo ionization detectors, infrared point sensors, catalytic-type gas detectors, ultrasonic sensors, electrochemical gas sensors, and semiconductor sensors are all common types of gas sensors (Yonghui Deng, 2019). All these sensors are used for a various application, with Infrared sensors and catalytic sensors used for measurement of combustible gases, while Electrochemical sensors and Metal Oxide Semiconductors for measurement of toxic gases. In a home the most likely gases to be detected are combustible gases.

1. **Infrared Point Sensors:** A point sensor based on non-dispersive infrared sensor technology is known as an infrared point sensor. The source of infrared radiation, the detector capable of seeing the radiation, and the channel between the detector and the source open to the gas to be detected are the key components of an infrared (IR) gas detection system (Alex et al., 2019). The Energy from the sensor beam is absorbed at a specified wavelength, based on the properties of the specific gas, in infrared (IR) point sensors. This wavelength's energy is compared to that of a wavelength outside of the absorption range. The difference in wavelengths between these two is proportional to the amount of gas present (Alex et al., 2019).

For self-compensation of variations in alignment, light source intensity, and component efficiency, dual source and dual receivers are used. Two infrared sources' transmitted beams are overlaid on an internal beam splitter. The gas measuring path carries 50% of the overlapping sample and reference signal, which is reflected to the measuring detector. The presence of combustible gas reduces the intensity of the sample beam, but not the reference beam, with the difference between the two signals proportional to the gas concentration in the measurement path. The other half of the overlapped signal is sent to the compensating detector through the beam splitter. The compensation detector keeps track of the intensity of the two infrared sources and compensates for any long-term drift automatically. Figure 2.4 illustrates the structure of a typical infrared point gas detector, and an IR signal analysis is represented in bar charts.

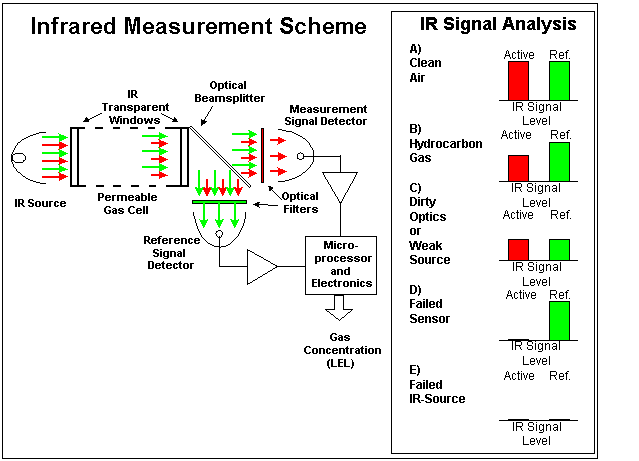


Figure 2.4: Measurement Scheme of an Infrared Point Sensor (Jose et al., 2017)

1. **Catalytic Sensors:** Catalytic sensors make up a substantial percentage of gas detectors on the market today. This method works by using catalytic oxidation to identify flammable gases like hydrocarbons. Catalytic oxidation is an oxidation process that uses a catalyst to convert organic molecules to carbon dioxide and water. A catalyst is a substance that speeds up the rate of a reaction while remaining relatively unchanged during the reaction (Jose et al., 2017). As combustible gas hits the catalytic surface, it is oxidized, and the wiring resistance is modified by the heat emitted. Catalytic sensors consist of two beads wrapped in platinum wire coil - a reference bead and an active bead with thermal barrier between the two beads. The resistance change, which is related to the measure of gas concentration, is commonly indicated by a bridge circuit. The catalytic sensor measuring principle is shown in Figure 2.5.

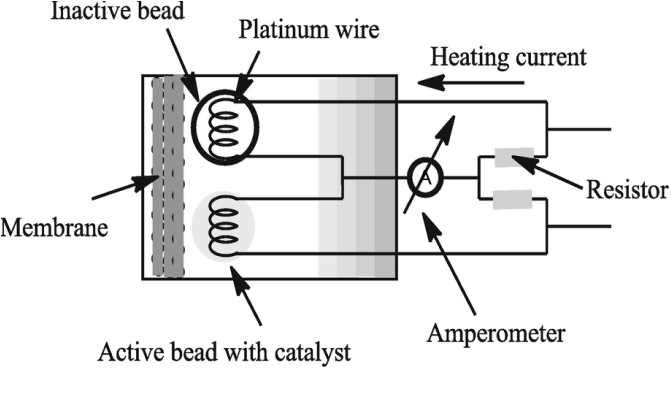


Figure 2.5: Catalytic Sensor Measuring Principle (Hassan *et al.,*, 2020).

The output of the sensor is proportional to the rate of oxidation. The signal's greatest output occurs around the stoichiometric (relating to substances in the exact proportions required for a certain reaction) gas combination, or it is based on the theoretical combustion reaction formula ( Ritter et al., 2018). Methane for example in Equation 2.2:

(2.2)

In order for the theoretical combustion to take place, one part of methane will require ten parts of air. The signal output of a methane sensor will respond linearly from 0 to 5 percent methane. The signal grows fast as the concentration approaches the stoichiometric value of around 9% and peaks about 10%. As the gas concentration hits approximately 20%, the signal begins to rapidly diminish; after 20%, it drops straight down to a level that shows no output as the gas concentration reaches 100%. (Ritter et al., 2018). Figure 2.6, illustrates this effect.

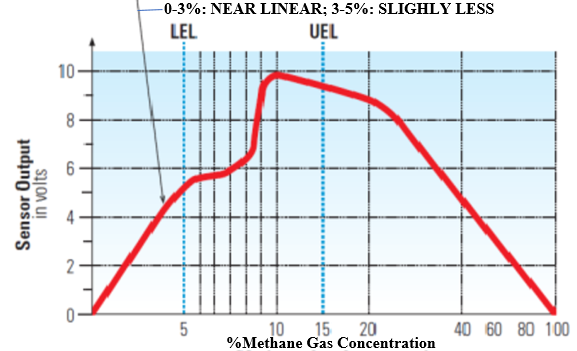


Figure 2.6: Sensor output Versus Methane Gas Concentration (Zaman et al., 2018)

2.2.1.4 *Smoke Detector*

A smoke detector detects smoke as a warning sign of a fire. Smoke detectors come in a variety of shapes and sizes and are commonly fashioned like a disk. According to Zaman et al. (2018), there are two types of smoke detectors:

1. Smoke detector with photoelectric technology (optical)

2. Smoke detector with ionization (physical)

1. **Photoelectric Smoke Detectors:** A photoelectric (optical) smoke detector works using light scattering principle. It works by shining a small light source into the dark sensing chamber, which could be an incandescent bulb or a light emitting diode (LED). A photoelectric receiver is a light-sensitive electrical component found in the light sensing chamber (typically a photodiode), as illustrated in Figure 2.7.

Because the light source and the light-sensitive electronic sensor are at a 90-degree angle, the light from the light source on the left usually streams straight across and misses the sensor. When smoke particles scatter light, some of it reaches the sensor, triggering a response (Hassan et al., 2020).

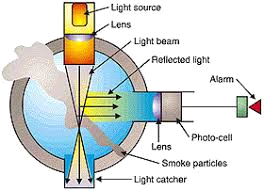


Figure 2.7: Optical Smoke Detector (Mike, 2015)

**2. Ionization Smoke Detectors:** An ionization smoke detector detects smoke by utilizing an ionization chamber and an ionization source. There is a miniscule amount of radioactive americium-241 inside the ionization detector. Americium, a radioactive element with a half-life of 432 years, is an excellent source of alpha particles. The radioactive material's alpha particle ionizes the oxygen and nitrogen atoms in the air in the chamber. The negative electron is attracted to the plate with positive voltage, and the positive atom is attracted to the plate with negative voltage. The electronics in the smoke detector senses the small amount of electrical current that those ions and electrons moving towards the plate represent (Zaman et al., 2018)

Figure 2.8 illustrates the working principle of an ionization sensor.

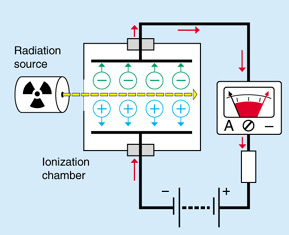


Figure 2.8: Principle of Ionization Chamber (Kamal et al., 2015)

Electrostatic attraction causes smoke particles to attach to ions in the ionization chamber if the air includes smoke. The ions do not shed their electric charge because of this, but the average mass of the charged particles in the chamber increases since the smoke particles are rather massive in comparison to the ionized air molecules. These particles must have the same average thermal energy as the surrounding air since they are still in thermal equilibrium with it (Kamal et al., 2015). Considering thermal energy in a gas is proportional to , if the ions' average mass m increases, their average speed must drop for their thermal energy to remain unchanged. The smoke detector is triggered by a decrease in measured current, which is caused by a fall in average speed (Kamal et al., 2015).

To “fast –flame” fires, an ionization alarm will often respond 30 to 90 seconds faster than a photoelectric smoke alarm. Ionization alarms, on the other hand, respond 15 to 50 minutes slower than photoelectric alarms in smouldering fires (Kamal, 2015).

2.2.2 Control Section

The control panel is the nerve centre of the installed intelligent home security system, and it is where all activities are supposed to occur. It is where all the security detection devices send their signals, as well as where answers are delivered to the security system peripherals as needed.

### 2.2.2.1 *Arduino Controller*

The Arduino UNO board, which includes an ATmega328 microprocessor, lies at the heart of the system. The ATmega328 is an integrated circuit (IC) that contains all the major components of a computer, including:

1. Processor
2. Memories
3. Peripherals
4. Inputs and outputs (Bayle, 2018)

The Arduino UNO is a microcontroller board that may also serve as a microweb server and the interface for all of the hardware components. The board serves as the hub for all communication and control in this system. The Arduino UNO contains 14 digital input/output pins, six of which can be used as PWM outputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an In-Circuit Serial Programming (ICSP) header, and a reset button. It comes with everything you'll need to get started with the microcontroller. Figure 2.9 show the image of an Arduino UNO board.

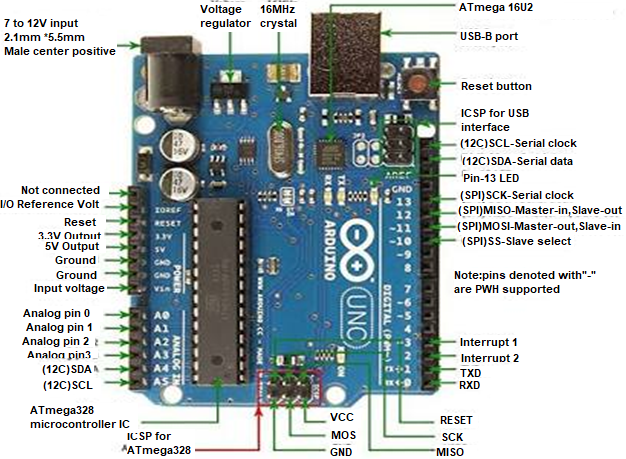


Figure 2.9: Arduino UNO Board (alldatasheet.com, 2019)

The ATmega 328 is an 8-bit CMOS microcontroller with a low power consumption based on the improved Reduced Instruction Set Computer (RISC) architecture. The ATmega328 delivers throughputs approaching 1 Million Instructions Per Second (MIPS) per MHz by executing strong instructions in a single clock cycle, allowing the system to be built to maximize power consumption versus processing performance. Figure 2.10 shows a block diagram of the internal architecture of the ATmega 328 microcontroller.

The microcontroller ATmega 328 has features like (Atmel AVR, 2019):

1. An operating voltage of 5V
2. Input voltage of about 7V-12V
3. 14 digital I/O pins (of which 6 provide PWM output)
4. 6 analog input pins
5. Flash Memory of 32KB
6. SRAM of 2KB

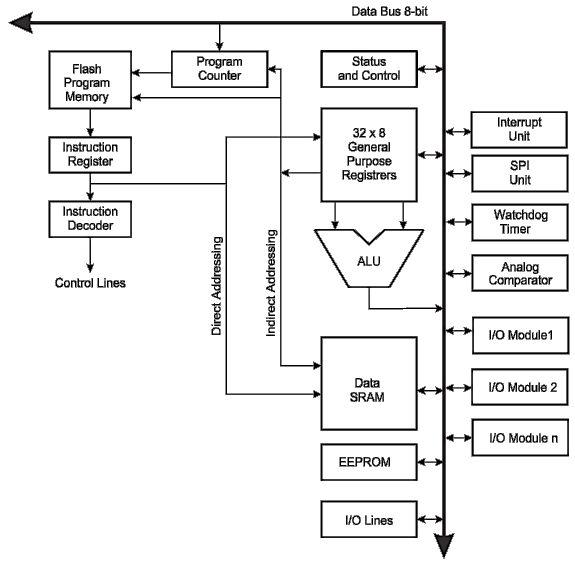


Figure 2.10: Block Diagram of the Internal Architecture of ATmega 328 IC

(alldatasheet.com 2019)

The Arduino UNO can be driven either by a USB connection or by an external power supply. The power source is automatically selected. An AC-to-DC adapter or a battery can provide external (non-USB) power. A 2.1mm centre-positive plug can be plugged into the board's power jack to connect the adapter. Battery leads can be put into the power connector's Gnd and Vin pin headers.

1. Input and Output

Using the pinMode(), digitalWrite(), and digitalRead() routines, each of the UNO's 14 digital pins can be utilized as an input or output. They are powered by 5 Volts. Each pin includes a 20-50k Ohm internal pull-up resistor (disconnected by default) and can deliver or receive a maximum of 40 mA. Furthermore, several pins have unique functionality:

1. Serial: 0 (RX) and 1 (TX): For receiving (RX) and transmitting (TX) TTL serial data, respectively.
2. External Interrupts: Pins 2 and 3 can be set to initiate an interrupt on a low value, a rising or falling edge, or a value change.
3. PWM: 3, 5, 6, 9, 10, and 11: The analogWrite function provides an 8-bit PWM output.

### LED: 13: Digital pin 13 has a built-in LED linked to it. The LED is turned on when the pin is HIGH, and the LED turned off when the pin is LOW.

### 2.2.2.2 *GSM/GPRS Module*

GSM When compared to Code Division Multiple Access (CDMA), the Global System of Mobile Communication is the most popular and widely utilized cell phone standard (CDMA). GSM (Global System for Mobile Communications) is an open and digital cellular system that transmits mobile voice and data services on quad-band frequencies (Rahman Zia, 2017). GSM owns a largest share of the world’s digital cellular subscribers. Almost 200 countries and about 5 billion people are using it as a phone today (Tech & Telecoms, 2018).

General Packet Radio Service (GPRS) is a packet-oriented mobile data service that supports data transfers over 2G, 3G, and 4G cellular communication systems in the worldwide system for mobile communications. GSM gets a packet data air interface and an IP-based core network with GPRS (Olarenwaju at al., 2017). GPRS is used on phones for a variety of data applications, including wireless internet (WAP), MMS, and internet-connected software.

The SIM800 is a module that provides calls, sends messages, text messages and even internet connections. The module is meant to be transportable, however extra peripherals are needed to work appropriately. Figure 2.11 show the image of a SIM800 board.

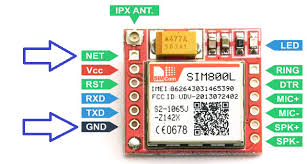


Figure 2.11: SIM800 Board (alldatasheet.com 2019)

Features of a typical module are as follows (alldatasheet.com 2019):

1. The SIM800 module contains 68 Surface Mount Technology (SMT) pads, which provide all hardware connections between the module and the customer's boards.

2. One full-featured UART port that may be split into two separate serial ports.

3. One USB port can be utilized for software upgrades and debugging.

4. A microphone input and a receiver output are included in the audio channels.

5. General-purpose input and output that can be programmed.

6. There is just one SIM card interface.

7. Bluetooth functionality is supported.

8. It is quad-band and can connect to any GSM network worldwide using any 2G SIM card.

9. AT command interface with detection of "auto baud"

10.Send and receive SMS messages, send and receive GPRS data (TCP/IP, HTTP, etc.)

The software communication module ensures proper conditioning of the activities and expected performance of all the hardware that makes up the intelligent home security system.

The Arduino module would be programmed via the Arduino IDE.

### *2.2.2.3 Smart Home Network*

The term wireless communication encompasses all kinds of connection and communication, using wireless communication technologies and devices, between the two or more devices using wireless signal. The advancement of wireless technology has translated to its advancements with effective features.

* + - 1. The transmission distances can range from a few meters to hundreds of kilometres.
      2. Cellular telephony, wireless internet access, wireless home networking, and other applications can all benefit from wireless communication.
      3. Cost-effectiveness, flexibility, ease, speed, accessibility, and continual connectivity are all advantages of wireless communication.

There are several conventions that are available for wireless communication for smart homes, common ones are Zigbee, WiFi, Insteon and Z-wave.

1. **Zigbee:** Zigbee is a wireless mesh network standard for low-cost, low-power devices used in wireless control and monitoring applications. Low-latency communication is provided via Zigbee. Typically, Zigbee chips are combined with radios and microcontrollers (Wang et al.,2014). Zigbee uses the industrial, scientific, and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide, though some devices use 784 MHz in China, 868 MHz in Europe, and 915 MHz in the United States and Australia; however, most commercial Zigbee devices for home use still use 2.4 GHz in those regions and countries. Data speeds range from 20 kbits per second (868 MHz band) to 250 kbits per second (2.4 GHz band).

For low-rate wireless personal area networks, Zigbee builds on the physical layer and media access control described in IEEE standard 802.15.4. (WPANs) (Wang *et al.,*2014). The network layer, application layer, Zigbee Device Objects (ZDOs), and manufacturer-defined application objects are all included in the specification. ZDOs oversee a variety of functions, including device role management, network request management, device discovery, and security (Danbatta and Varol, 2019). The ability to carry out secure communications, safeguard the establishment and transfer of cryptographic keys, ciphering frames, and control devices is another distinguishing characteristic of Zigbee. It is based on the IEEE 802.15.4 fundamental security architecture.

The Zigbee protocols are designed for embedded applications that require little power and can handle low data speeds.

1. **Insteon:** Light switches, lights, thermostats, leak sensors, remote controls, motion sensors, and other electrically powered equipment can all communicate with one other via power lines, radio frequency (RF) connections, or both. It uses a dual-mesh networking topology, in which all devices are peers and each send, receives, and repeats messages independently. It has been linked to the Internet of Things, just like other home automation systems.
2. **Z-wave:** Z-wave is a wireless technology that uses low-energy radio waves to enable smart devices and appliances to interact with one another. Z-Wave is a [wireless](https://en.wikipedia.org/wiki/Wireless) communications protocol used primarily for [home automation](https://en.wikipedia.org/wiki/Home_automation) It's a mesh network that communicates from appliance to appliance using low-energy radio waves, enabling for wireless management of home appliances and other devices including lights, security systems, thermostats, windows, locks, swimming pools, and garage door openers (Danbatta and Varol, 2019). A Z-Wave system, like other home and office automation protocols and systems, can be controlled remotely via the Internet and locally via a smart speaker, wireless keyfob, or wall-mounted panel, with a Z-Wave gateway or central control device serving as both the hub controller and portal to the outside.
3. **WIFI:** Wi-Fi is a term that refers to a group of radio technologies that are often used to connect devices across a wireless local area network (WLAN). It is based on the IEEE 802.11 standard family. The ESP8266 WiFi Module is a self-contained (System-on-Chip) SoC with an inbuilt TCP/IP protocol stack that can provide access to your WiFi network to any microcontroller. The ESP8266 may either host an application or offload all Wi-Fi networking functionality to a separate application processor (Wang et al.,2014). Each ESP8266 module comes with an AT command set software pre-installed, allowing it to connect to an Arduino device. This module has a powerful enough on-board processing and storage capability to allow it to be integrated with sensors and other application-specific devices via its GPIOs with minimal up-front implementation and minimal runtime loading. Its high on-chip integration allows for minimum external circuitry, and the front-end module is designed to take up as little PCB space as possible. Figure 2.12 shows a diagram of a WiFi Module.

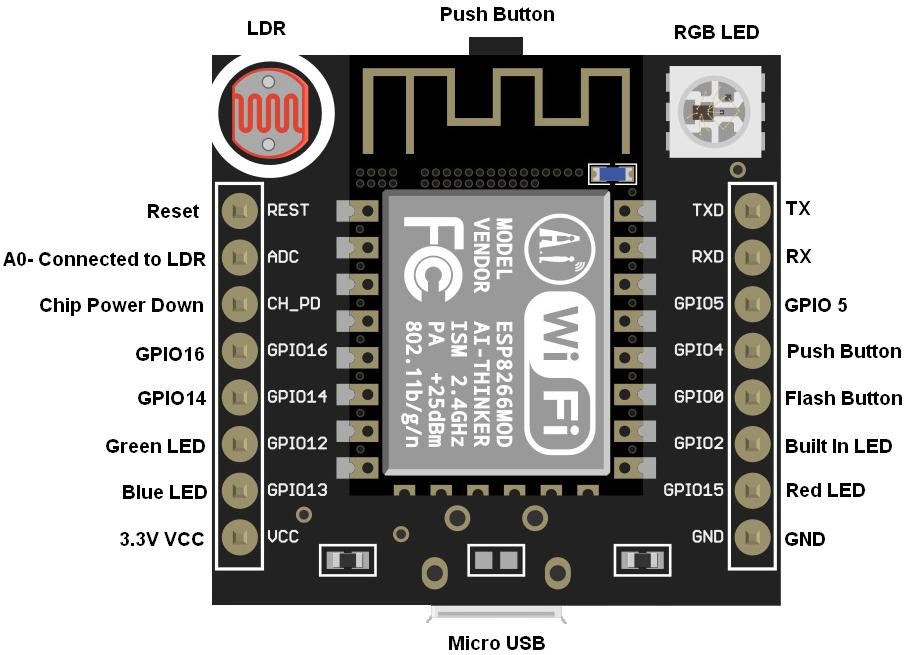


Figure 2.12: WiFi Module (alldatasheet.com 2019)

### 2.2.2.4 *Arduino Software IDE*

The Arduino UNO is made up of a physical programmable circuit board (microcontroller) and software (called an IDE) that runs on a computer and is used to create and upload computer code to the physical board.

The Integrated Development Environment (IDE) is open-source software provided by an Italian company called Smart Project. The tool can run on windows, Mac OS, X, and Linux. The programming language used for communication in Arduino UNO is a wiring-based language which is similar in style C/C++ language (Balye, 2018). It comes with a code editor that offers text cutting and copying, text search and replacement, automatic indenting, brace matching, and syntax highlighting, as well as simple one-click procedures for compiling and uploading applications to the Arduino board. A text space, a text terminal, a toolbar with buttons for common functions, and a hierarchy of operating menus are all included. The GNU General Public License, version 2 is used to license the IDE's source code.

2.2.3 Electronic System Reliability

Reliability is defined as “the possibility that a piece of equipment functioning under specified environments shall perform adequately for a given period of time”. Reliability index of an equipment is usually given between 1 and 0 (Akinola, 2017).

### *2.2.3.1 Predicted Reliability of a System*

To simplify the computation of predicted reliability of an electronic system, several steps are involved which includes system subdivision, drawing of reliability model and failure analysis (Akinola, 2017).

There are three prerequisites in calculation of predicted system reliability, which include system subdivision, reliability model and system unit relations (Akinola, 2017).

1. **System Subdivision:** The first step in calculating the reliability of a large system is to break it down into pieces that are small enough to be analysed individually.
2. **Reliability Models:** Reliability diagrams are handy tools in system behaviour predictions. This model shows functional relationships between each unit, showing their effects on system performance.
3. **System Units’ Relations:** System unit relation can be series, parallel or mixed. In series systems, failures in any of the units causes system failure. The necessary probability is the likelihood that component 1 to component n will develop a problem within the specified time frame. The summing rule is used to find the combined probability if the constituent probabilities are not mutually inclusive (Akinloa, 2017). Summation of their individual probabilities as given by equation 2.5.

P = (2.5)

In parallel systems usually, redundancy is practiced. Introducing the use of more equipment than the minimum required, so that failure in a unit does not ground the whole system, normally switching mechanism is implemented to enable faulty subsystem to be disconnected. It is simple to compute the chance of failure in a parallel system than it is to compute reliability explicitly. Because the components are linked in parallel, a system failure can only occur if all of the subsystems fail. The probability (Ps) is calculated as the product of the failure probabilities in each of the subsystems over a particular time interval (Akinola, 2017), system reliability R can be gotten from the relation in equation 2.6.

R = 1 – Ps (2.6)

Most electronic systems are mixed systems, with both series and parallel units, arrangement is frequently used where some part of the system is particularly prone to failure.

*2.2.3.2 Reliability Prediction for Electronic Systems*

Reliability prediction techniques are numerous. They are usually classified into five main categories (Micheal, 1999):

* 1. Similar system techniques: To assess the level of reliability, the system under test is compared to another similar system with a known dependability value.
  2. Similar Complexity Techniques: The planned system's dependability is estimated by comparing its complexity to that of another known reliable system of similar complexity.
  3. Function-based prediction: To anticipate the reliability of a novel design, correlations between function and reliability are studied.
  4. Part Count Techniques: Reliability can be approximated as a relationship between the components units used in the system design.
  5. Stress Analysis Techniques: The failure rate is a function of individual part failure rates, considering operating stress, individual part rating features, and part type (Warrendale, 1987).

## 2.3 Review of Similar Works

This section includes a review of other researchers' similar work. The reviews are conducted with the goal of determining the scope of work carried out in the implemented research field.

**Mutlag *et al.,* (2013)** created a smart surveillance monitoring hardware solution that included a Raspberry Pi and a PIR sensor. The system was created using digital signal processing and image processing concepts. This device included a Raspberry Pi that operated and controlled the device, as well as a motion detector and a live video stream that was captured for later replay. When motion was detected, a pi camera took a photo and sent it by SMS to the owner's smartphone, with a copy recorded on the server. Image processing was a benefit of the security system. A system that takes action only based on motion detection, on the other hand, is prone to a high number of false alarms. This system could be enhanced by adding more surveillance-related sensors, which would lessen the risk of false alarms, which was one of the work's limitations.

**Potts and Sukittanon, (2013)** implemented a home security system, exploiting Bluetooth and Android mobile devices. The implemented system used Bluetooth as a wireless connection protocol which allowed a user to lock or unlock a door at a short range from the door. The advantage of the Bluetooth technology which featured wide compatibility, low power consumption, low cost and security was used a major focus in the designed work. The design called for an Android Smartphone with Bluetooth capabilities and a microcontroller security interface. The security interface consisted of Arduino Mega 2560 microcontroller and a Bluetooth transceiver. The mobile device was able to communicate approximately 10m away from the microcontroller. The implemented work made life easier for people with disability. The short-range limitation in which the system worked effectively was the reason for improvement requirement of this work.

**Bangali and Shaligram (2013)** GSM-based smart home security system was built and implemented, the system recommended two methods of home protection. The first system used a web camera, which gives a security alarm in the form of sound and sends an SMS to the homeowner anytime there is motion in front of the camera. When a fire incident happens, the second technique sends SMS using a GSM/GPS module (Sim548c) and an Atmega 644p microcontroller. The installed system is designed to keep the house safe from intruders and fires. The focus is on security of the home when the user is away from home. The implemented system gives the advantage of effectiveness and low cost in terms of both capital and running cost. However, a system designed to be effective only when the home users are away does not cover a fundamental requirement of a security system, which is to protect homeowners and their properties from danger either when at home or away.

**Huang *et al.,* (2014)** implemented a remote home security based on wireless sensor network and GSM technology. The system was implemented by applying WSN and GSM technology. It can detect theft, leaking raw gas and fire. The hardware of the system includes TC35 GSM module, CC1100 transceiver, and a single chip C8051F310 microcontroller. The system software was implemented in C51 language. The C51 language is a special form of C language used to program the 8051 series of microcontrollers. The system structure was composed of the Microcontroller Unit based wireless control center, one WSN center node module, and several data collecting nodes, a GSM module, and a mobile phone. The system prototype was tested and it worked perfectly. The system presented a solution for establishing a low power consumption remote home security alarm system. However, the system can only give indications in form of alarms and messages, it also has no control capabilities incorporated in it and cannot be communicated to remotely by the homeowner.

**Chandramohan *et al*., (2015)** presented an intelligent smart home automation and security system using Arduino and Wi-Fi. With the help of an integrated micro-web server with internet protocol (IP) connectivity for access and to manage equipment and devices remotely via an Android-based smart phone app, the installed system provided for flexible home control and monitoring. In comparison to similar systems, the implemented system does not require a dedicated server PC and provides a new communication protocol for monitoring and controlling the home environment, which includes more than just switching functionality. For communication between the remote user and the home device, the new circuit architecture is implemented in a silent based web services in an interoperable application layer. The communication path available for use in this system is the internet without any other option. This single communication path indicates a rigid communication path which is a major hindrance to accessibility of the security system.

**David et al., (2015)** created a home automation system based on Arduino that provides a low-cost, adaptable solution for house control and environmental monitoring. It uses an Arduino Mega 2560 microcontroller with an inbuilt micro-web server and IP connectivity to access and control gadgets and appliances remotely. A web application or a Bluetooth Android-based Smart phone app can be used to operate these devices. In comparison to existing systems, the system does not require a dedicated server PC and uses a revolutionary communication protocol to monitor and control the home environment beyond simple switching. The use of a Wi-Fi shield as a Micro web server for the Arduino eliminates the need for wired connections between the Arduino board and any computer, lowering costs and allowing it to function as a stand-alone device. Improving this system will include adding certain security features as well as expanding the system's control choices to include SMS and phone alerts.

**Sohog and Ahmed, (2015)** developed and executed a home security system that is more convenient, versatile, and affordable. The microcontroller is at the heart of the system. This system consists of a PIR sensor, an Android application, an ATmega8 microcontroller, a Bluetooth module (HC-05), and a cloud-based application that allows the user to watch their home in real-time from any location through the Internet. This system also has an alarm feature. A cloud system was developed to be connected to through an android application. Homeowner’s connection to the security system is through their phone and via SMS. The implemented systems depend largely on the viability of internet service. In places where the cost of internet is high, the purpose of such security system is defeated which is a limitation of this work.

**Isa and Sklavos (2016)** designed and implemented a smart home automation with GSM security system. The designed system was implemented on a microcontroller module, though an embedded platform. The system operated on different level of user’s access control, based on password policy. The system sends an alert when intrusion through the door is suspected. The system, compared with related integration in the field, stands out in its low cost and the fact that it was designed as an open system, allowing the user to add any additional sensors or coding functionalities. The limitations of this system are the fact that the security system is only activated when an intruder tries to gain entry though the door, leaving other possible access point unsecured, and security threats are indicated in form of SMS only.

**Abel A. Zandamela (2017)** designed a smart home security system using Arduino board. The system was designed based on internet of things technology. The system was designed using Mega 2560 Arduino board, board platform and other sensors. The smart home security system has the capability of sensing intrusions, temperature and fire outbreak. The system gave indications in the form of sound when a security or safety breach occurred. A multitasking security system should include a remote alerting system. However, the designed system lack ability to communicate with its user remotely.

**Jara *et al.,* (2017)** developed and deployed a panic button system for community security in Ecuador-rural pucara's districts. When one of the panic buttons is touched by VirtualPrivate Network (VPN), the Security system uses the Raspberry Pi Zero to send, a remote alarm to the Security Services system. The low cost of this alarm system makes it accessible to the poor, as well as its stability in the event of an emergency, the panic button system has the purpose of delivering security and tranquillity to the rural areas. The system provided a solution to the lack of service coverage of mobile networks that does not allow the monitoring of the area, and implemented a stable communication channel, which allowed the transmission of emergency signals in real time. Three buttons are used to deal with emergencies in the management of fire, health and safety incidents. The moment a button receives an event, the system will determine the type of emergency and transmit the signal to the security institution, which will dispatch the specialized personnel for emergency care. However, a system of this nature can only be useful in a very small community, given that the exact location of emergency is not covered, the possibility to ascertain the authenticity of an event of security concern is not covered.

**Jewel *et al.,* (2017)** designed and implemented a versatile and intelligent home security system. The system was implemented based on microcontroller to alert when an unauthorized person tries to enter the home, though SMS and Buzzer. To make the system more secure, security devices such as an android-based door password, a manual keyboard to open the door, PIR motion to detect unauthorized people around the home, a rotating ultrasonic sensor activated by a servo motor to activate the camera to capture images, and an RF transceiver to produce an audio signal to alert people outside the home were included. All sensor outputs were monitored by an Android phone that was connected to the microcontroller via Bluetooth. The sensor will be activated if someone tries to unlock the system. The controller portion receives a pulse and activates the devices such as the GSM module, LCD display, camera, RF Transceiver, and buzzer. This system can be improved by incorporating additional paths by which the system can communicate in case of intrusion like calls, and e-mails, also a possibility of a two-way communication between the security system and the homeowner.

**Abu *et al.,* (2017)** developed a home security system using Internet of Things with online database server, FAVORIOT. Sensors (passive infrared and infrared) are used to monitor presence of intrusion if any. Blynk application is used as a switch to switch system, the user maintains an unlimited control access of the system. The data received from the sensor was sent to the microcontroller which was already equipped with an internet module. The system was built to give indications in form of SMS alert. This system was implemented on a software platform. However, a system designed to be effective only on software application can easily be compromised and will not be reliable in places where the internet service is expensive or unreliable.

**Olanrewaju *et al.,* (2017**) An autonomous home security system based on GSM technology and an embedded microcontroller unit was conceived and built. The study took advantage of the GSM network, mobile module, and electronic circuit to create an automated system that can function as a standalone device. Long-range connectivity and sophisticated coordinating software with a database storing the user's essential mobile information are the system's highlights. When an incursion is detected, the GSM-based security system responds quickly to sensors and sends an SMS. Additional communication options for the system in case of intruder detection, like phone call and e-mail, will improve the robustness of the security system, and the ability to remotely access the security system.

**Qasim *et al.,* (2019**) designed and implemented a home security system monitored by using wireless sensor networks (WSN) and internet of things (IOT). The system was implemented using microcontrollers. The system used Raspberry Pi to enable cloud technology, nRF24L01 for radio signal transfers and Arduino UNO for sensors controls. The paper presented a secure home based on IoT where several activities are being sensed and monitored. Specifically, liquefied gas, humidity, body temperature and motion. The implemented system communicated effectively between sensors and sent SMS when intrusion was detected, or a safety breach was suspected. Also in the system is a camera for live streaming to a registered email address, in case of intrusion. Highlights of the system are long range of communication and robust coordinating software with a database containing the user required mobile information and email address. However, with several redundant sensors, the system cost runs high. A cost-effective system will ensure wide acceptance, and in extension mitigate home insecurity to an appreciable extent.

**Syafeeza *et al.*, (2020)** designed and developed a prototype for a IoT based facial recognition door access control home security system using Raspberry Pi. The developed system is to secure the home by facial recognition and door control features. The system was implemented by applying deep learning and cloud technology. In case of an unauthorized visitor the system sounds a buzzer and sends an alarm message including a face capture of the intruder remotely to saved contacts on the database. The hardware of the system includes Raspberry Pi, a camera, and few passive components. The bulk of the system development is with the software. Convolutional Neutral Network (CNN) was the algorithm used for the aspect of the system’s deep learning, Blynk was used for cloud technology, and Python was used for programming the micro-controller. The system presented a solution for establishing remote home security alarm system with some problems associated with authentication mitigated. However, it requires a large memory space for its database, which directly affects the product cost and power consumption.

A lot of study has been done on home security systems, as evidenced by the studied literatures. Some of the implemented systems are of limited communication range. With most restricted to only one means of communication, from the security system to the homeowner, implying lack of flexibility in means of communication and the absence of two-way remote communication option and obviously some on the high financial side.