VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELAGAVI-590 018, KARNATAKA

ARKA Educational & Cultural Trust

JAIN INSTITUTE OF TECHNOLOGY

Davanagere-577003, KARNATAKA

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

PRE-FINAL YEAR B.E. (2022 – 2023)

Mini Project Report
On

" IOT BASED INTRUDER DETECTION SYSTEM "

UNDER THE GUIDANCE OF

Mrs. PUSHPALATHA O

Assistant Professor, Dept. of ECE

J.I.T. , Davanagere

MINI PROJECT ASSOCIATES

Abdul Majeed Kaif N	4JD20EC001
Bharath B J	4JD20EC004
Mohammed Sanaulla	4JD20EC027
Akhilesh V Desai	4JD21EC400

ABSTRACT

An IOT-based intruder detection system involves the use of various sensors and communication protocols to detect and report unauthorized access to a particular area. The system comprises of multiple components, including sensors, microcontrollers, and a cloud-based platform for data storage and analysis. The primary function of the system is to monitor the presence of unauthorized individuals in a particular area and generate alerts to the user or a security team. The sensors used in the system could be passive infrared (PIR) sensors, door and window sensors, or magnetic sensors. The sensors are connected to a microcontroller, which acts as a gateway between the sensors and the cloud-based platform.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

An IOT-based intruder detection system is a security system that can detect and notify you of any unauthorized entry into your home or workplace using IOT devices. This system uses a combination of sensors, microcontrollers, and wireless communication technologies to monitor the environment and detect any unusual activity.

The system can be configured to trigger an alarm or send notifications to a mobile device or email address when an intruder is detected. This can provide a quick and effective way to prevent theft or damage to property.

To build an IOT-based intruder detection system, you will need to select the appropriate sensors, such as motion sensors or door and window sensors, and connect them to a microcontroller, such as an Arduino or Raspberry Pi. You will also need to set up a wireless network, such as Wi-Fi or Bluetooth, to enable communication between the sensors and the microcontroller.

Figure 1.1 Intruder Detection System

1.1 PROBLEM STATEMENT

Many households and businesses need an efficient and reliable way to monitor their premises and detect intruders. Traditional intruder detection systems often rely on sensors and cameras that are connected to a centralized monitoring system, which can be expensive to install and maintain. IOT-based intruder detection systems offer a cost-effective and scalable solution to this problem. Hence in the proposed system designing and implementing requires addressing various challenges, including selecting the right sensors, developing a reliable communication network, integrating with existing systems, and ensuring secure data transmission.

1.2 OBJECTIVES

The objectives of an IOT-based intruder detection system may vary depending on the specific needs and requirements of the project. However, some common objectives of such a system may include:

- **Detecting:** The primary objective of the system is to detect the presence of an intruder.
- **Alerting**: Alert the owner or authorized personnel in real-time.

This will help to prevent the intruder from causing any harm or damage.

1.3 MOTIVATION

The motivation behind the project of an IOT-based intruder detection system is to provide enhanced security and protection for homes, offices and other premises. This system can provide peace of mind for owners as they can be alerted to any suspicious activity even when they are away from home.

CHAPTER 2

LITRETURE SURVEY

- Khushbu H Mehta, Niti P Guptahave (2016) [1] presented real time monitoring and security system using Raspberry Pi the system allow user to live monitor from any place. In the system Authors have discuss that if motion is detected it will check for face detection if the face is detected it will stored on local storage, they have used background subtraction Algorithm for face detection. Authors concluded that system is able to identify faces and user can able to monitor remotely.
- Sowmiya. U, Shafiq Mansoor. J. (2015) [2] have developed an Raspberry Pi based home door security through 3g dongle to connect any door with internet, in this system user also implemented PIR sensor and camera. PIR sensor used for detecting person and camera used for capturing the video of person comes at door. The video will be send through 3g dongle to authorised person. They have also discussed some advantages of this system. They have concluded use of this system like bank, hospital etc.
- Harikrishnan G.R. et. al. (2015) [3] have implemented home automation and security system in this system user can continuously monitor home from remote location if the intruder detected system will generate alarm and captures the image of the intruder and the captured image will be send to owners mobile through SMS, WhatsApp, Call, E-mail. They have discussed few advantages of this system. Authors have concluded that this system is useful for securing commercial places.
- N. Komninos et. al. (2014) [4] surveyed the opportunities and drawbacks that exists in smart home security and smart grid. They have listed all the treats in the survey. The survey also shows the way using the energy in an effective and efficient manner. Suggestion also provided to prevent and the defenses against various attacks.

CHAPTER 3

METHODOLOGY

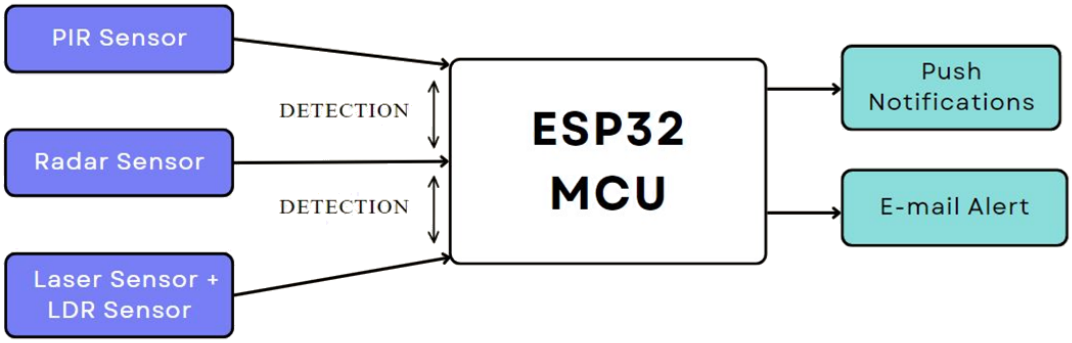


Figure 3.1 Block Diagram of Intruder Detection system

In this block diagram, the ESP32 is responsible for processing data from the different sensors, including PIR sensor, laser module, microwave radar sensor, temperature and humidity sensor, and piezoelectric sensor. The SMS/Call module is used to alert the user of any intruder detection through SMS or call. The alarm module is used to produce an audible alarm when an intrusion is detected.

The Intruder Detection block is responsible for detecting any intrusion activity by processing the data from the different sensors. The ESP32 then sends the alert to the SMS/Call Module to notify the user of the intrusion. The Alarm Module is activated to produce an audible alarm to deter intruders and alert nearby individual

CHAPTER 4

HARDWARE AND SOFTWARE REQUIREMENTS

4.1 HARDWARE REQUIREMENTS

- ESP32 MICROCONTROLLER
- PIR Sensor (HC-SR501)
- LASER MODULE and LDR
- MICROWAVE RADAR SENSOR (RCWL-0516)

4.1.1 ESP32 MICROCONTROLLER

- ESP32 is a dual-core XTensa LX7 MCU, capable of running at 240 MHz. Apart from its 512 KB of internal SRAM, it also comes with integrated 2.4 GHz, 802.11 b/g/n Wi-Fi and Bluetooth 5(LE) connectivity that provides long-range support. It has 45 programmable GPIOs and supports a rich set of peripherals.

4.1.2 INTRODUCTION TO ESP32 BOARDS:

- The ESP32 microcontroller board is a versatile and powerful development platform that has gained significant popularity in the world of embedded systems and Internet of Things (IOT) applications. It is based on the ESP32 system-on-a-chip (SOC) designed by Espressif Systems, a leading semiconductor company. The ESP32 board combines a dual-core processor, wireless connectivity options, and a rich set of peripherals, making it a suitable choice for a wide range of projects. It features two 32-bit Xtensa LX6 microprocessor cores, which can be clocked up to 240 MHz, offering substantial computational power for demanding tasks.

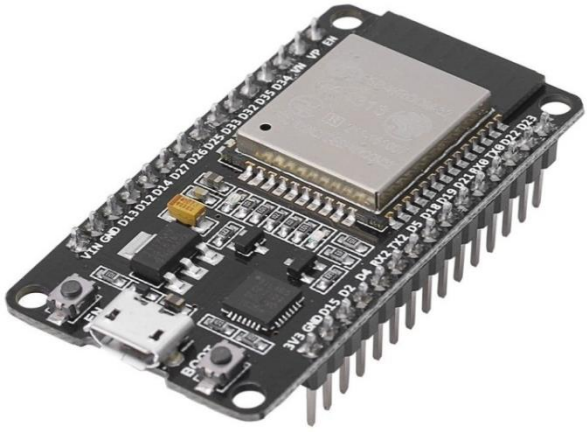


Figure 4.1 ESP32 MICROCONTROLLER

- One of the standout features of the ESP32 is its comprehensive wireless capabilities. It supports Wi-Fi, both 2.4 GHz and 5 GHz bands, allowing seamless connectivity to local networks or the internet. Additionally, it includes Bluetooth Low Energy (BLE) support, enabling communication with other devices and peripherals in energy-efficient ways. The ESP32 board also offers a multitude of interfaces and peripheral options, including GPIO (General Purpose Input/Output) pins, I2C, SPI, UART, ADC, DAC, and more. These interfaces enable easy integration with various sensors, actuators, displays, and other components, facilitating the development of complex and interactive projects.

4.1.3 COMPONENTS OF ESP32 BOARDS:

- Pin Description of ESP32 Microcontroller board as shown in below Figure

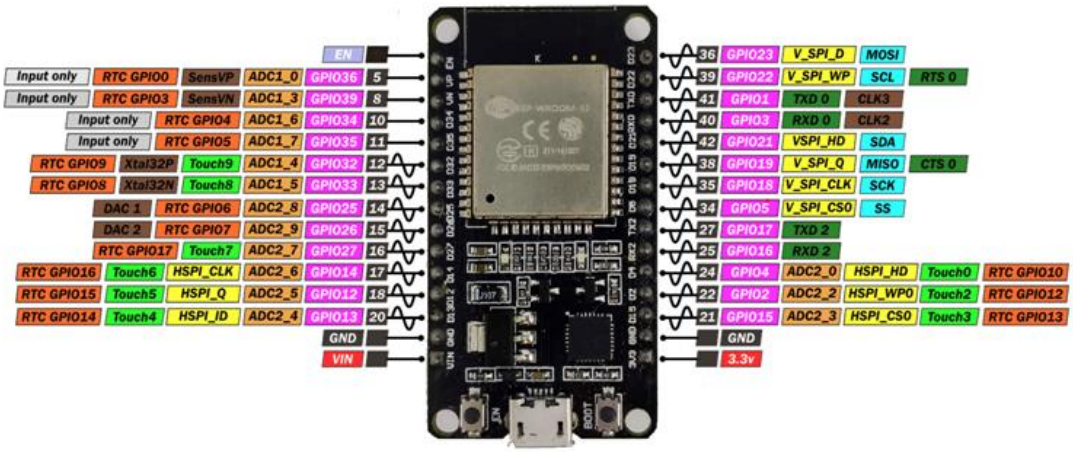


Figure 4.2 Pin Description of ESP32 Microcontroller Board

Functional Description of the Pins:

- **GPIO Pins**: General Purpose Input /Output pins used for digital input/output operations. They can be configured as digital input or output, and some pins have additional functionality such as PWM, I2C, SPI, etc.
- **Analog Input Pins**: These pins allow analog voltage measurements using the built-in ADC (Analog-to-Digital Converter) of the ESP32. They can measure voltages ranging from 0 to 3.3V.
- **UART Pins**: Universal Asynchronous Receiver/Transmitter pins used for serial communication. They enable the board to communicate with other devices using protocols such as RS-232, RS-485, or MIDI.
- **I2C Pins**: Inter-Integrated Circuit pins used for connecting the ESP32 to I2C-compatible devices like sensors and displays. I2C allows for multiple devices to be connected on the same bus using only two wires (data and clock).
- **SPI Pins:** Serial Peripheral Interface pins used for high-speed synchronous serial communication between the ESP32 and peripheral devices like sensors, displays, and memory chips. SPI supports full-duplex communication and can connect multiple devices using chip select lines.
- **PWM Pins**: Pulse Width Modulation pins used to generate analog-like signals with varying duty cycles. These pins are often used to control the brightness of LEDs, control motor speed, or generate audio signals.
- **DAC Pins:** Digital-to-Analog Converter pins used to generate true analog voltage signals. They provide a higher resolution for analog output compared to PWM pins.
- **RTC GPIO Pins**: These pins can be used for various purposes, including deep sleep wake-up sources, external interrupt inputs, or pulse counter inputs.
- **Touch Sensor Pins**: The ESP32 has built-in touch sensor support, and these pins are used to connect touch-enabled electrodes or capacitive touch sensors.
- **ADC Reference Voltage Pins**: These pins are used to set the reference voltage for the ADC. They allow you to select the voltage range for analog measurements.
- **Power Supply Pins**: These pins provide power to the ESP32 board. They include VCC (3.3V or 5V), GND (Ground), and VIN (Voltage Input) for external power supply.
- **LED Pins:** These pins are typically connected to LEDs on the board, which can be used for status indication or custom use.

4.1.4 PIR Sensor (HC-SR501)

The HC-SR501 is a passive infrared (PIR) sensor module that is commonly used to detect motion in a given area, and it operates at a voltage of 5V DC, with a detection range of up to 7 meters and a detection angle of 120 degrees. The sensor module is designed to operate within a wide voltage range, typically between 4.5V and 20V DC. This makes it compatible with various microcontrollers and development boards that provide 3.3V or 5V logic levels.

Figure 4.3 PIR SENSOR

4.1.5 HC-SR501 PIR Sensor Functional Description

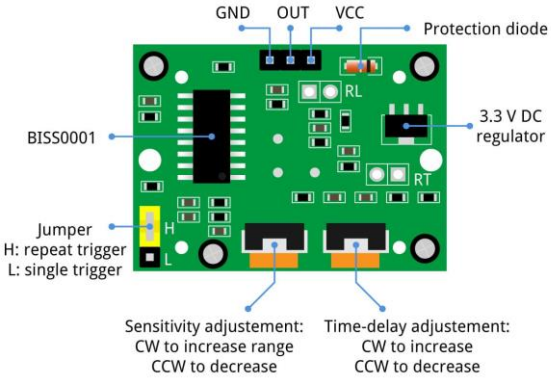


Figure 4.4 Pin Description of PIR SENSOR(HC-SR501)

- **Working Principle**: The HC-SR501 PIR Sensor detects motion by sensing changes in infrared radiation emitted by objects in its field of view. It uses a pyroelectric sensor to detect variations in the infrared heat signature caused by moving objects.
- **Sensing Range**: The sensor has an adjustable sensing range, typically ranging from a few meters up to approximately 7 meters. The detection range can be adjusted using the onboard potentiometers to suit specific application requirements.

- **Output Signal**: The sensor provides a digital output signal indicating the presence or absence of motion. It has a built-in comparator circuit that processes the sensor input and produces a digital HIGH (3.3V or 5V) signal when motion is detected and a digital LOW signal when no motion is present.
- **Operating Voltage**: The HC-SR501 PIR Sensor operates on a wide range of voltages, typically between 4.5V and 20V DC. It is designed to work with microcontrollers and development boards that provide 3.3V or 5V logic levels.

4.1.6 LASER MODULE and LDR

A laser module is a compact device that produces a highly focused beam of light, known as a laser beam. The module consists of several key components, including a laser diode, a collimating lens, and a control circuit.

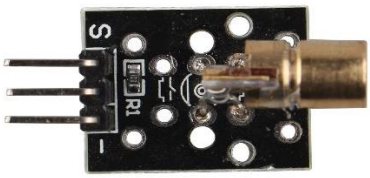


Figure 4.5 Laser Module

The 5mm LDR (Light Dependent Resistor), also known as a photoresistor, is a type of sensor that detects changes in light intensity. It is commonly used in various applications that require light sensing and control.

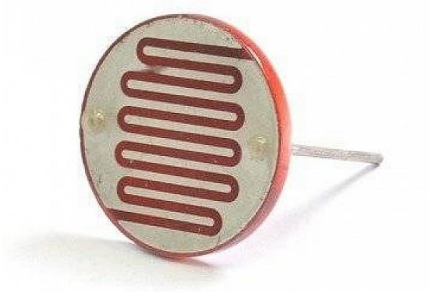


Figure 4.6 LDR(Light Dependent Resistor)

The 5mm LDR consists of a semiconductor material that exhibits a varying electrical resistance based on the amount of incident light. When exposed to light, the resistance of the LDR decreases, and when in darkness, the resistance increases.

To use the 5mm LDR, it is typically connected as a voltage divider circuit with a fixed resistor. The varying resistance of the LDR causes a corresponding change in the voltage across it, which can be measured using an analog input of a microcontroller or an ADC (Analog-to-Digital Converter). The measured voltage can then be used to determine the light intensity in the environment.

4.1.7 MICROWAVE RADAR SENSOR (RCWL-0516)

Microwave radar sensors typically operate in the frequency range of 24 GHz to 77 GHz.

The maximum detection range of a microwave radar sensor depends on the frequency, power, and antenna design, but ranges up to several hundred meters are possible. The field of view of a microwave radar sensor depends on the antenna design and can vary from a few degrees to more than 100 degrees.

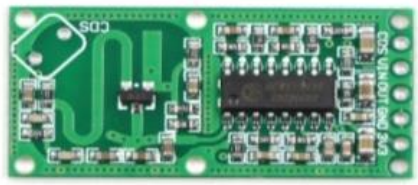


Figure 4.7 Microwave Radar Sensor

- **Radar Principle**: The RCWL-0516 operates based on the Doppler radar principle. It emits continuous low-power microwave signals and detects the frequency shift caused by the motion of objects within its detection range.
- **Sensing Range**: The sensor has a typical detection range of a few meters, which can be adjusted using the onboard potentiometer.
- **Operating Frequency**: The RCWL-0516 operates at a frequency of around 3.2 GHz, in the microwave frequency range.

4.2 SOFTWARE REQUIREMENTS

The Software version we have used here is ARDUINO IDE 2.1.1 .

4.2.1 ARDUINO IDE 2.1.1

The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. This software can be used with any Arduino board. Arduino is the computer hardware and software device. Arduino UNO ATmega328 offers UART TTL-serial communication, and itis accessible on digital pins like TX (1) and RX (0). The software of an Arduino has a serial monitor that permits easy data. There are two LEDs on the board like receiver and transmitter which will blink whenever data is being broadcasted through the USB. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, for loading programs from personal computers. The microcontrollers are mainly programmed using a dialect of features from the programming languages Embedded C, C and C++.

Figure 4.8 ARDUINO IDE 2.1.1 Software

CHAPTER 5

WORKING AND IMPLEMENTATION

This project involves creating an intruder detection system using PIR, radar, and laser sensors. The main component of the system is the ESP32 Wi-Fi module. The sensors are connected to the ESP32 microcontroller, which receives data from the sensors and controls the system.

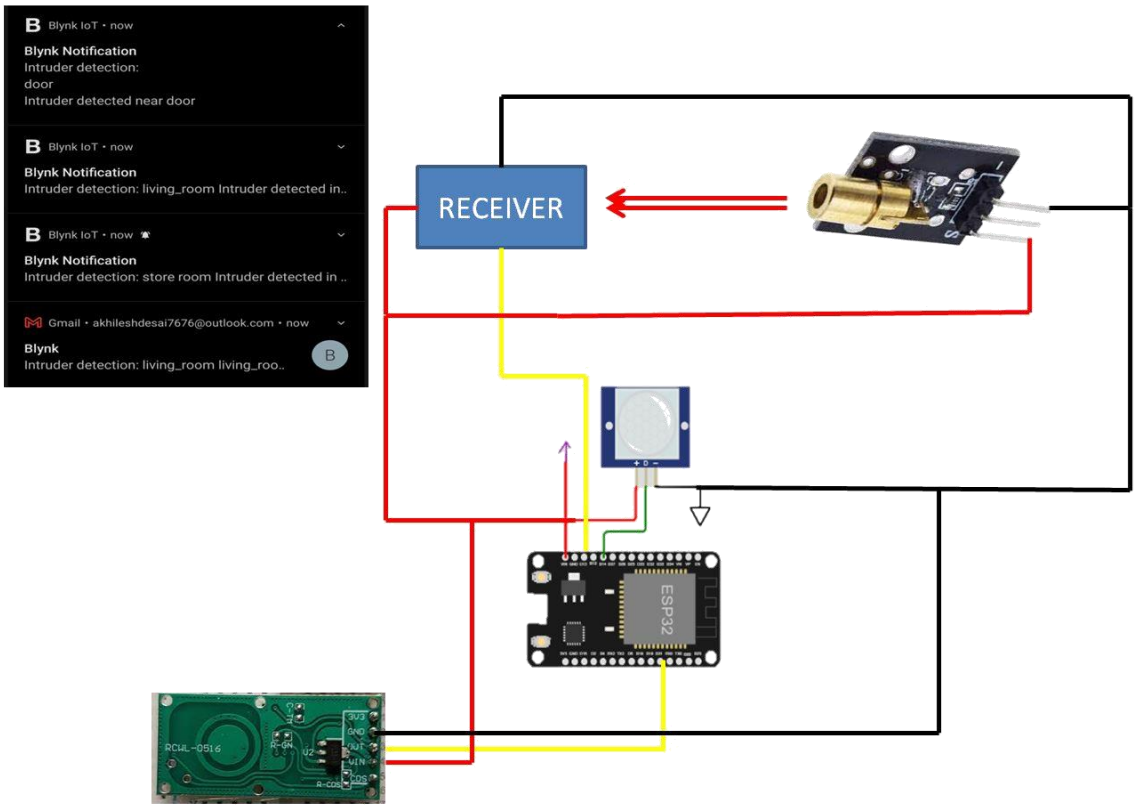


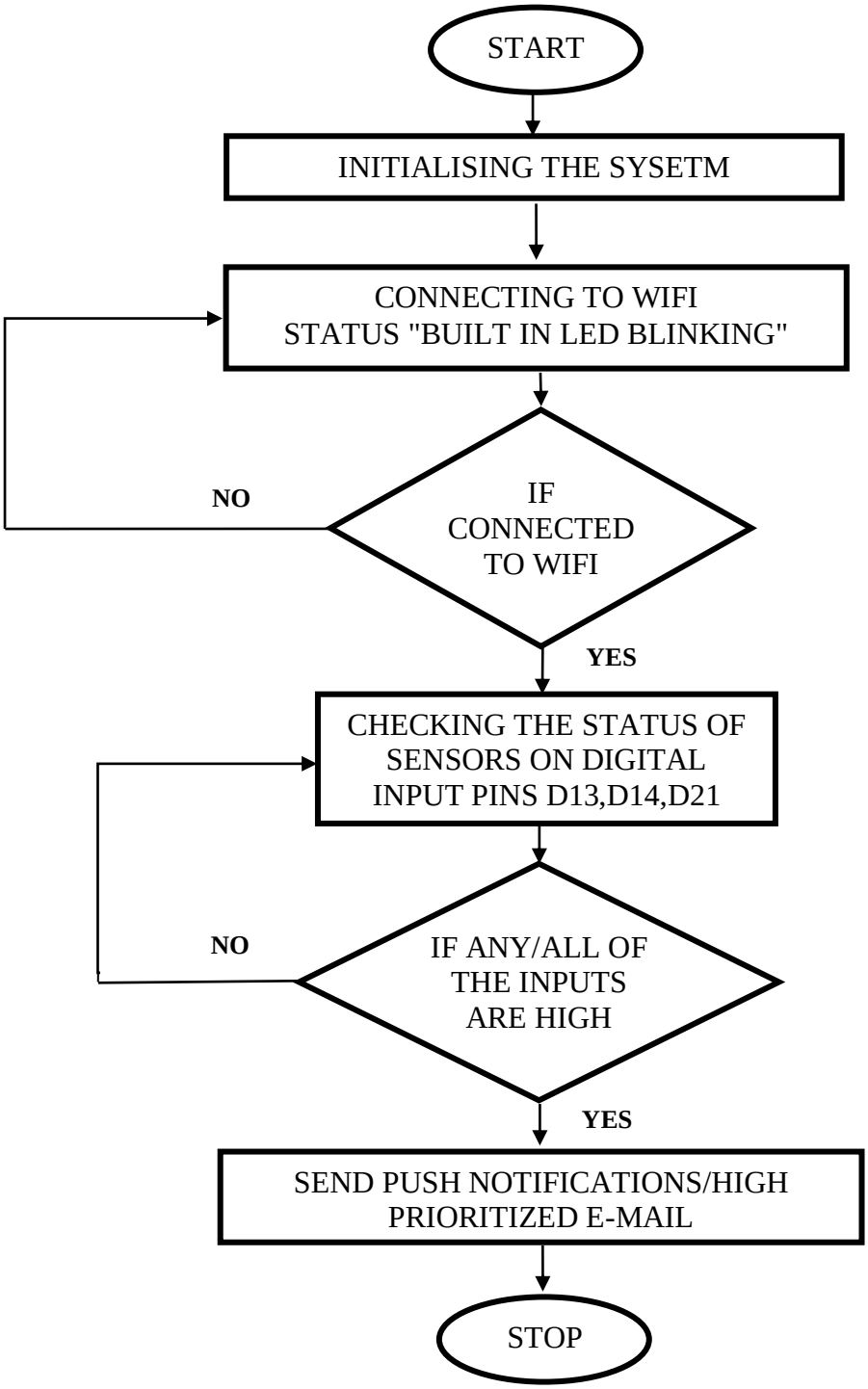
Figure 5.1 Implementation Diagram

The PIR sensors detect motion using infrared technology, while the radar sensors use radio waves to detect movement. The laser sensors act as a light source for the LDR (Light Dependent Resistor), which detects changes in light intensity. This information is sent to the microcontroller.

The microcontroller is programmed to display messages when an intruder is detected in different areas of the house. For example, if an intruder is detected in the store room, the microcontroller will show a message indicating this. Similar messages can be displayed for the living room and the door area.

In addition to displaying messages, the microcontroller can send notifications to a mobile device using the Blink IOT app. This app is widely recognized and trusted for IOT projects. By following the programming code provided (version 2.1.1), you can interface the ESP32 microcontroller and set up the system to receive notifications on your mobile device.

FLOWCHART



CHAPTER 6

RESULTS

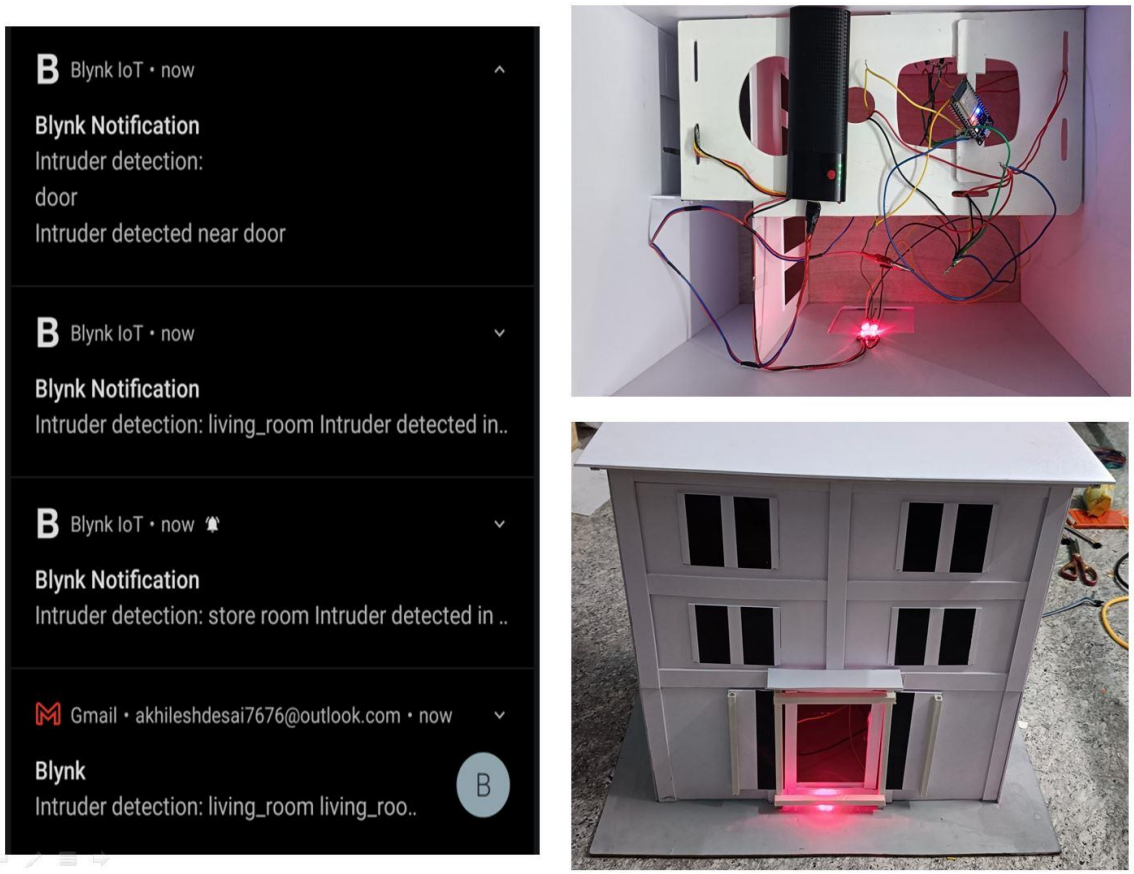


Figure 6.1 Output When Intruder Is Detected

If any intruder enters into the home or any place where our "Intruder detection system" is installed then one gets an immediate alert to their mobile through push notifications. Hence they get to know about the intrusion. The push notifications serve as real-time alerts to the user, notifying them about the intrusion as soon as it happens. This enables the user to be aware of the situation and take necessary actions, such as contacting the authorities or taking measures to ensure their safety.

CHAPTER 7

ADVANTAGES AND DISADVANTAGES

7.1 ADVANTAGES

- **Real-time monitoring**: An IOT-based intruder detection system can provide real-time monitoring of a premises. This means that the system can detect any intrusions immediately and alert the user through various means such as SMS, email, or push notifications.
- **Cost-effective**: Compared to traditional security systems, an IOT-based system can be much more cost-effective. The use of low-cost sensors, wireless communication, and cloud computing can significantly reduce the cost of the system.
- **Easy installation**: An IOT-based intruder detection system is typically easy to install, as it requires minimal wiring and infrastructure. The system can be set up quickly and easily, without the need for specialized technical expertise.
- **Integration with other systems**: An IOT-based system can be integrated with other IOT devices, such as smart locks, lighting, and thermostats, to create a comprehensive home automation system. This can provide additional security and convenience to the user.

7.2 DISADVANTAGES

- **Complexity**: IOT systems can be complex and require specialized knowledge and expertise to develop and implement. If you don't have experience with IOT systems, you may find that the learning curve is steep and the process is time-consuming.
- **Maintenance**: IOT systems require ongoing maintenance and updates to ensure that they remain functional and secure. This could require a significant investment of time and resources over the long term.

CHAPTER 8

APPLICATIONS

1. **Home security**: An IOT-based intruder detection system can be used to secure homes against break-ins. The system can be installed in doors, windows, and other entry points to detect any unauthorized access.

2. **Office security**: IOT based intruder detection systems can be used in offices to protect against theft and unauthorized access. The system can be used to monitor sensitive areas such as server rooms, and alert security personnel in case of a breach.

3. **Warehouse security**: An IOT-based intruder detection system can be used to secure warehouses against theft and unauthorized access. The system can be used to monitor entry points, and alert security personnel in case of a breach.

4. **Vehicle security**: An IOT-based intruder detection system can be used to secure vehicles against theft. The system can be used to monitor doors, windows, and other entry points, and alert the owner in case of a breach.

5. **Agricultural security**: IOT based intruder detection systems can be used in farms to protect against theft of crops and livestock. The system can be used to monitor the perimeter of the farm, and alert the owner in case of a breach.

6. **Industrial security**: An IOT-based intruder detection system can be used in industrial facilities to secure against theft of materials and equipment. The system can be used to monitor entry points, and alert security personnel in case of a breach.

CHAPTER 9

CONCLUSION AND FUTURE SCOPE

The intruder detection system based on IOT offers a valuable solution for enhancing security in various settings. By leveraging interconnected devices, sensors, and network connectivity, the system effectively detects unauthorized access and alerts the relevant parties in real-time. This technology provides a proactive and efficient approach to safeguarding premises and assets, minimizing the risk of security breaches. Implementing an IOT-based intruder detection system can greatly enhance security measures and contribute to a safer environment.

- ## FUTURE SCOPE

The future scope for an IOT-based intruder detection system project can involve several advancements and potential improvements. Here are some simple future scope ideas:

Machine Learning and AI Integration: By incorporating machine learning and artificial intelligence techniques, the intruder detection system can learn from patterns and behaviors to differentiate between normal activities and suspicious actions. This can help in reducing false alarms and improving the overall accuracy of the system.

Video Surveillance Integration: Integrating the intruder detection system with video surveillance cameras can provide visual evidence of the intrusion. This integration can enable live streaming of video footage and recording of suspicious activities, which can be useful for identifying intruders or analyzing security breaches later.

REFERENCES

1. Khushbu H Mehta, Niti P Gupta, “Vision Based – Real Time Monitoring Security System for Smart Home”, Vision Based – Real Time Monitoring Security System for Smart Home, Vol. 4, Issue 2, February 2016 ISSN(Online): 2320-9801 ISSN (Print): 2320-9798

2. Sowmiya U, ShafiqMansoor.J., “Raspberry Pi based home door security through 3g dongle”, International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015,ISSN 2091-2730

3. Harikrishnan G.R., Noufal V.P., Latheesh S., “Third Eye -An Efficient Home Security Automation System”, International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 17, May 2015

4. N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures", IEEE Communications Surveys & Tutorials, Volume: 16, Issue: 4, pp. 1933 - 1954, 2014.