An Internship Project Report

On

Bank security System

Submitted in partial fulfilment of the requirements for the award of the degreeof

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING –

ARTIFICIAL INTELLIGENCE&MACHINE LEARNING

BY

A. SHINY PAVITHRA	**22NN1A4253**
CH. BHAVYA	**22NN1A4206**
A. AMRUTHA	**22NN1A4203**
CH. ANITHA	**22NN1A4208**

Under the Esteemed Guidance of

Mr. G. Manidheer

Assistant Professor, CSE-AIML

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-

ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

VIGNAN'S NIRULA INSTITUTE OF TECHNOLOGY AND SCIENCE FOR WOMEN

PEDAPALAKALURU, GUNTUR-522005

(Approved by AICTE, NEW DELHI and Affiliated to JNTUK, KAKINADA)

(2022-2023)

VIGNAN'S NIRULA INSTITUTE OF TECHNOLOGY AND SCIENCE FOR WOMEN

PEDAPALAKALURU, GUNTUR-522005

(Approved by AICTE, NEW DELHI and Affiliated to JNTUK, KAKINADA)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the internship project report entitled **"Bank Security System"**, is a Bonafide work of **A.Shiny Pavithra(22NN1A4253), Ch. Bhavya(22NN4206), Ch. Anitha (22NN1A4208) and A.Amrutha(22NN1A4203)** submitted to the faculty of Computer Science And Engineering-Artificial Intelligence & Machine Learning, in the requirements for the award of degree of **BACHELOR OF TECHNOLOGY** in **COMPUTER SCIENCE AND ENGINEERING-ARTIFICIAL INTELLIGENCE & MACHINE LEARNING** from **VIGNAN'S NIRULA INSTITUTE OF TECHNOLOGY AND SCIENCE FOR WOMEN, GUNTUR.**

Project Guide

Mr.G.Manidheer

Assistant Professor CSE-AIML

HEAD OF DEPARTMENT

Ms.P.SilpaChaitanya

EXTERNAL EXAMINER

DECLARATION

We hereby declare that the work described in this Internship project report, entitled **"Bank Securtiy System"** which is submitted by us for the award of **Bachelor of Technology** in the Department of **Computer Science and Engineering-Artificial Intelligence & Machine Learning** to the **Vignan's Nirula Institute of Technology and Science for women**, affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, is the result of work done by us under the guidance of **Ms. M. Anusha , Assistant Professor, CSE-AIML**.

The work is original and has not been submitted for any Degree/ Diploma of this or any other university.

Place:

Date:

A.Shiny Pavithra	**22NN1A4253**
Ch.Bhavya	**2NN1A4206**
Ch.Anitha	**22NN1A4208**
A.Amrutha	**22NN1A4203**

ACKNOWLEDGEMENT

We express our heartfelt gratitude to our beloved principal **Dr. P. Radhika** for giving a chance to study in our esteemed institution and providing us all the required resources.

We would like to thank **Ms.P.Silpa Chaitanya, Assistant Professor, Head of the Department of Computer science and Engineering-Artificial Intelligence & Machine Learning**, for his extended and continuous support, valuable guidance and timely advices in the completion of this project thesis.

We wish to express our profound sense of sincere gratitude to our Project Guide **Mr.G.Manidheer Assistant Professor** without whose help, guidance and motivation this project thesis could not have been completed the project successfully.

We also thank all the faculty of the Department of Computer Science and EngineeringArtificial Intelligence & Machine Learning for their help and guidance of numerous occasions, which has given us the cogency to build-up adamant aspiration over the completion of our project thesis.

Finally, we thank one and all who directly or indirectly helped us to complete our project thesis successfully.

PROJECT ASSOCIATES

A.Shiny Pavithra	**(22NN1A4253)**
Ch.Bhavya	**(22NN1A4206)**
Ch.Anitha	**(22NN1A4208)**
A.Amrutha	**(22NN1A4203)**

ABSTRACT

Security is primary need for every person whether it just comes to physical things or digital data. Banks are one of those places where security plays a major role. Banks hold financial resources and sensitive information. Physical security, such as having individuals monitor the bank premises, is one way to ensure safety. Additionally, other methods can be employed that do not rely on human surveillance.

This project aims to provide a means of safeguarding the bank from theft without the need for direct human supervision. The project utilizes a laser and infrared sensor to detect the presence of any objects or individuals in the vicinity of the bank and triggers an alert by sounding a buzzer whenever an intrusion is detected.

INDEX

CHAPTER-1

CHAPTER-2

CHAPTER-3

CHAPTER-4

CHAPTER 1

INTRODUCTION

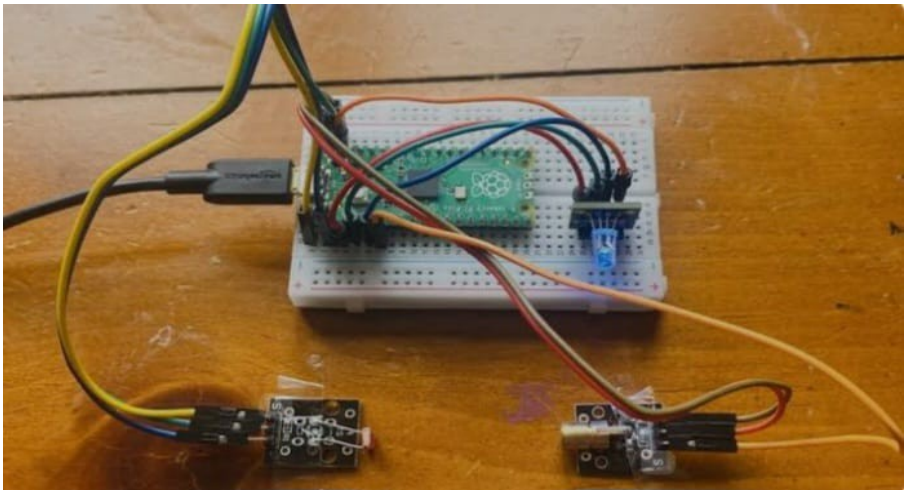
1.1 Introduction to project

The word LASER stands for Light Amplification by Stimulated Emission of Radiation. These are available in different types like semiconductor, infrared, GaAs laser diode. This has an energy wavelength of approximately 900 nanometres with a beam divergence of 3 million radians i.e. equal to a beam width small beam width.

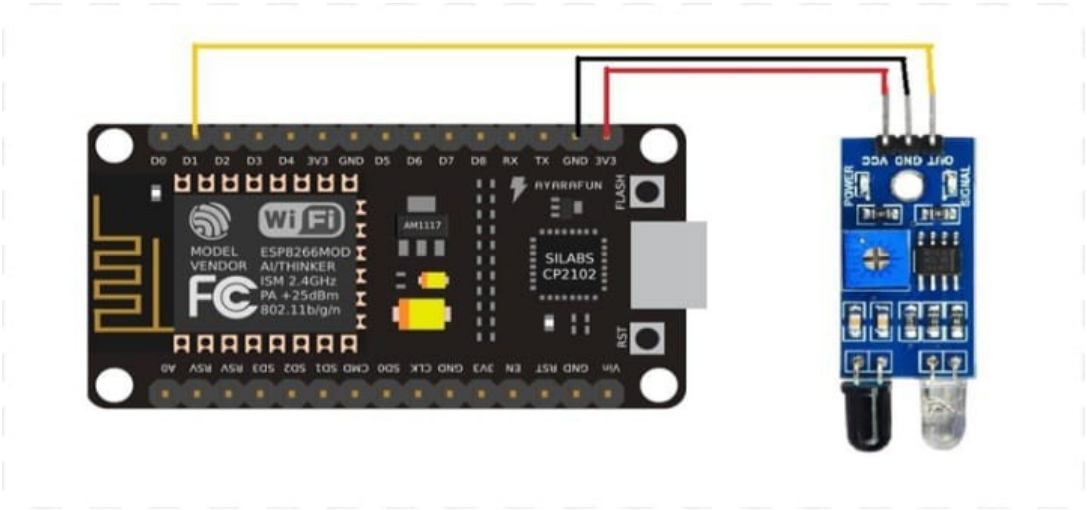
Laser technology products will calculate distance by measuring the time of flight of very short pulses of infrared light. It is different from the traditional surveying instrument method of measuring phase shifts by comparing the incoming wavelength with the phase of the outgoing light pulse.

The Laser security systems are high tech innovations Laser based Security system is a type of security and alarm system that uses laser light and a LDR sensor (Light Dependent Resistor). A security System protects our banks from intrusion and unauthorized access.

A Laser Security system can act as standalone system, which makes some sound or noise when it detects any irregular activity.



IR based security system is also a part of this project. This IR based security system contains a IR sensor which helps us in object detection.



The circuit is based on obstacle detection when a person or a thing comes in between the transmitter and receiver. The alarm gets triggered and beeps continuously till the time the circuit is reset.

1.2 Introduction to Embedded System

An embedded system is a computer system that is designed to perform a specific task or set of tasks. It is a combination of computer hardware and software that is integrated into a larger system. Embedded systems are used in various applications such as home appliances, transportation, healthcare, business sector & offices, defence sector, aerospace, and agricultural sector. The three main components of an embedded system are hardware, software, and firmware. Hardware refers to the physical components of the system such as microprocessors or microcontrollers.

Software refers to the programs that run on the hardware. Firmware is a type of software that is embedded in the hardware and is responsible for controlling the system. An Embedded system is a special- purpose system in which the computer is completely encapsulated by or dedicated to the device or system it controls. Unlike a general-purpose computer, such as a personal computer, an Embedded System performs one or few predefined Tasks usually with very specific requirements. Since the system is dedicated to specified tasks, design

engineers can optimize it, reducing the size and cost of the product. Embedded Systems are often mass- produced, benefiting from economies of scale.

Characteristics of Embedded System:

• An embedded System is any computer system hidden inside a product other than a computer.

• Throughput – Our system may need to handle a lot of data in short period of time.

• Response – Our system may need to react to events quickly.

• Test ability- Setting up equipment to test embedded software can be difficult.

• Debug ability- Without a screen or a keyboard, finding out what the software is doing wrong is a troublesome problem.

• Reliability – Embedded Systems must be able to handle any situation without human intervention.

• Memory Space - Memory is limited on Embedded Systems, and you must make the software and the data fit into whatever memory exists.

• Power Consumption – Portable systems must run on battery power, and the software in these systems must conserve power.

• Processor hogs- Computing that requires large amounts of CPU time can complicate the response problem.

1.3 Introduction to IOT

INTERNET OF THINGS (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate Interaction amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically away people lead their daily lives. Advancements in medicine, power, gene therapy agriculture, smart cities, and smart homes are just a very few of the categorical example where IoT is strongly established.

IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data. With more than 7 billion connected IOT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. Oracle has a network of device partners.

The most important features of IoT on which it works are connectivity, integrating, active engagement, and many more. Connectivity refers to establish a proper connection between all the things of IoT platform it may be server or cloud. After connecting the IoT devices, it needs a highspeed messaging between the devices and cloud to enable reliable, secure and bi-directional communication. IoT makes things smart and enhances life through the use of data. For example, if we have a coffee machine whose beans have going to end, then the coffee machine it orders the coffee beans of your choice from the retailer. The most important features of IoT on which it works are connectivity, analysing, integrating, active engagement, and many more. Some of them are listed below:

Connectivity: Connectivity refers to establish a proper connection between all the things of IoT platform it may be server or cloud. After connecting the IoT devices, it needs a high speed messaging between the devices and cloud to enable reliable, secure and bi-directional communication.

Analysing: After connecting all the relevant things, it comes to real-time analysing the data collected and use them to build effective business intelligence. If we have a good insight into data gathered from all these things, then we call our system has a smart system.

Integrating: IoT integrating the various models to improve the user experience as well. Artificial Intelligence: IoT makes things smart and enhances life through the use of data. For example, if we have a coffee machine whose beans have going to end, then the coffee machine it orders the coffee beans of your choice from the retailer.

Sensing: The sensor devices used in IoT technologies detect and measure any change in the environment and report on their status. IoT technology brings passive networks to active networks. Without sensors, there could not hold an effective or true Iot environment.

Active Engagement: IoT makes the connected technology, product, or services to active engagement between each other.

Endpoint Management: It is important to be the endpoint management of all the IoT system otherwise, it makes the complete failure of the system. For example, if a coffee machine itself order the coffee beans when it goes to end but what happens when it orders the beans from a retailer and we are not present at home for a few days, it leads to the failure of the IoT system.

1.4 Need of IoT

The Internet of Things (IoT) stands as a transformative force, reshaping our interactions with the world and revolutionizing diverse aspects of our daily lives. At its core, IoT thrives on connectivity, fostering seamless communication between devices and promoting interoperability. Through automation, IoT enhances efficiency by enabling devices to operate autonomously based on predefined conditions or real-time data, reducing the need for constant human intervention. In the realm of smart cities, IoT contributes to urban development by introducing intelligent transportation systems, energy management, and sustainable practices, thereby enhancing overall quality of life. Health care benefits from IoT through wearables and remote monitoring tools, offering personalized insights and timely interventions. Industries leverage Industrial IoT (IoT) to optimize manufacturing processes, monitor equipment health, and implement predictive maintenance strategies, leading to increased productivity and cost savings. From smart homes with connected appliances to environmental monitoring and supply chain optimization, IoT's impact is far-reaching, creating a more connected, efficient, and intelligent world across various domain

CHAPTER -2
LITERATURE SURVEY

2.1 Introduction:

Bank security is a critical concern due to the high-value assets and sensitive information stored within these institutions. Traditional security measures, such as CCTV cameras, alarms, and security personnel, have been supplemented with advanced technologies, including laser and IR systems, to enhance security. As a result, bank security systems are continually evolving to address emerging threats and enhance safety measures. One of the advanced technologies being integrated into bank security is IR sensor & laser technology. Laser & IR sensor-based security systems offer several benefits, including high precision, reliability, and the ability to cover extensive areas without physical barriers. In this project, we used the Laser Diode Module KY-008 to design a Laser Light Security System using Arduino with Alarm. The idea behind the project is to build a security system. The buzzer alarm will begin to ring whenever any object blocks the LASER ray. This project can be implemented anywhere; in addition to buildings or other structures, it can also be used to secure other valuable items, priceless antiques in museums, etc. With the help of a LASER beam security system, many people secure their homes, offices, shops, warehouses, and other structures

2.2. Laser-Based Systems

In the rapidly evolving landscape of security technologies, banks are increasingly adopting laser-based security systems to safeguard their assets and ensure the safety of customers and staff. A bank security system using laser technology is a highly advanced and effective way to protect against unauthorized access and theft. The system utilizes laser beams to create an invisible grid that covers the entire perimeter of the bank, including doors, windows, and any other potential entry points. When an intruder attempts to breach the grid, the laser beam is interrupted, triggering an alarm. Laser technology offers precise, reliable, and non-intrusive methods for detecting and preventing unauthorized access and intrusions. Laser technology is widely used

in security systems due to its precision and reliability. The primary applications in bank security include perimeter security. Laser fences are invisible beams of laser light that form a virtual barrier. When an intruder crosses this barrier, the interruption is detected, triggering an alarm. By using this sound of alarm we can detect that something was wrong. When an intruder crosses a laser beam or disrupts a laser grid, the system immediately detects the breach . Upon detection of an intrusion, the system triggers an alarm, which can be audible. The alarm can also notify security personnel. Advanced systems can differentiate between actual threats and non-threatening movements (e.g., small animals), reducing false alarms.

2.3. Infrared Sensors Based Systems

Infrared (IR) sensors are increasingly being integrated into bank security systems to enhance the detection and prevention of unauthorized access. These sensors operate by emitting infrared light, which is invisible to the human eye, and detecting the reflection of this light from nearby objects. When an object or individual crosses the IR sensor’s path, the sensor detects a change in the reflected light pattern and triggers an alarm or security response. The use of IR sensors in bank security offers several advantages, including high sensitivity to movement, the ability to function in low light conditions, and the capacity for discreet installation. By leveraging this technology, banks can improve their surveillance capabilities, ensuring better protection of assets and heightened safety for both employees and customers. IR sensors are strategically placed at entry points, sensitive areas, and critical zones within the bank. These sensors are calibrated to detect specific movements and heat signatures that indicate the presence of an intruder. The IR sensor emits infrared light, which is reflected back when it hits an object or person. The sensor continuously monitors the intensity and pattern of the reflected IR light. When an unauthorized person crosses the sensor’s path, the pattern of reflected light changes. The sensor detects this disruption, indicating a potential breach. The detected change in the IR light pattern is converted into an electrical signal. This signal is processed by the sensor's onboard microcontroller to determine if the detected movement is legitimate or a false alarm.

II. LITERATURE REVIEW

A bank security system integrating laser and IR sensors offers a robust and multi-layered approach to detecting and preventing intrusions, providing a high level of accuracy and reliability. The laser sensors create an invisible grid that detects intruders, with adjustable sensitivity to detect specific types of breaches, such as glass breakage, and can be integrated with alarm systems and video surveillance. Meanwhile, IR sensors detect heat and motion within a specific range, ideal for areas where laser beams may be obstructed, and can be adjusted to reduce false alarms. When combined, the system provides comprehensive coverage, real-time alerts, and notifications, and can be customized to meet specific bank security requirements. While installation and calibration may be complex, and environmental factors like temperature and humidity may affect performance, regular maintenance and testing can mitigate these issues. Overall, this integrated system offers a valuable investment for banks and financial institutions, providing a strong deterrent against unauthorized access and theft, and ensuring the security of assets and customers. The utilization of laser technology in bank security systems represents a significant advancement in safeguarding financial institutions against unauthorized access and theft. Lasers, known for their precision and reliability, have been integrated into various security measures, enhancing the overall robustness of bank protection protocols. One primary application is in intrusion detection systems, where laser beams create an invisible barrier around secure areas. Any interruption of these beams triggers alarms, ensuring immediate response to potential breaches. Moreover, lasers are employed in biometric authentication systems, particularly in retina scanning, providing a highly secure method for verifying identities. The precision of laser technology allows for accurate and quick recognition, minimizing the risk of false positives and ensuring that only authorized personnel gain access. Additionally, the use of lasers in surveillance systems enhances the clarity and accuracy of monitoring, enabling high-resolution imaging that is crucial for identifying and tracking intruders. This integration of laser technology into bank security systems not only improves the detection and response mechanisms but also acts as a deterrent, significantly reducing the likelihood of attempted thefts or unauthorized entries. The

continuous advancements in laser technology promise further enhancements in security measures, potentially incorporating more sophisticated applications such as real-time threat analysis and automated response systems. Overall, the adoption of laser technology in bank security systems underscores the commitment of financial institutions to leverage cutting-edge innovations to protect assets and ensure the safety of their operations. The incorporation of infrared (IR) sensors in bank security systems has emerged as a pivotal advancement in enhancing the safety and integrity of financial institutions. IR sensors, known for their ability to detect heat and motion, offer a discreet and reliable means of monitoring and securing bank premises. One of the primary applications of IR sensors in bank security is in intrusion detection systems. These sensors are strategically placed to monitor for unauthorized entry by detecting the infrared radiation emitted by human bodies. When an intruder is detected, the system triggers alarms, alerts security personnel, and initiates other protective measures, ensuring a swift response to potential threats. Furthermore, IR sensors are utilized in conjunction with surveillance cameras to improve night vision capabilities, providing clear imagery even in low-light conditions. This enhancement is crucial for continuous monitoring and recording, ensuring that no suspicious activity goes unnoticed. Additionally, IR sensors play a vital role in access control systems. By incorporating IR technology into biometric devices, such as facial recognition or hand geometry scanners, banks can achieve higher accuracy in identifying and authenticating individuals, thereby preventing unauthorized access. The non-intrusive nature of IR sensors makes them an ideal choice for monitoring sensitive areas without causing disruptions to daily operations. Moreover, the integration of IR sensors with advanced analytics allows for real-time threat assessment and predictive security measures, enhancing the overall security strategy. As technology progresses, the potential for IR sensors in bank security systems continues to expand, with innovations such as thermal imaging and intelligent sensor networks paving the way for more sophisticated and proactive security solutions. Overall, the deployment of IR sensors in bank security systems reflects a strategic move towards leveraging advanced technology to safeguard assets, ensure operational continuity, and maintain the trust of clients.

CHAPTER-3
DESIGNED SYSTEM

3.1 Introduction

"A bank security system is a robust and multi-faceted framework designed to protect financial institutions, their customers, and assets from various threats. This comprehensive system integrates physical barriers, surveillance technologies, access control measures, alarm systems, secure storage solutions, network security protocols, and intelligent systems to detect and respond to potential security breaches. By implementing these measures, banks can prevent fraud, theft, and cyber attacks, ensuring a safe and secure environment for financial transactions and customer confidence."

The subject deals about banking and financial systems prevailing in a country. The banking system consists of Central banks, Commercial banks, Co-operative banks, foreign banks, etc., which are involved in the banking operations of the Country. The financial system deals about money market, capital market, foreign exchange market and the various sources for raising funds. It also includes financial instruments. With changing world trade, there has been a tremendous change, both in the banking and financial system. Added to this, the technological changes with the advent of computers have also brought in enormous changes in the functioning of banking and financial systems. New sources of credit have also emerged such as credit cards which even persons in the rural areas can avail of.

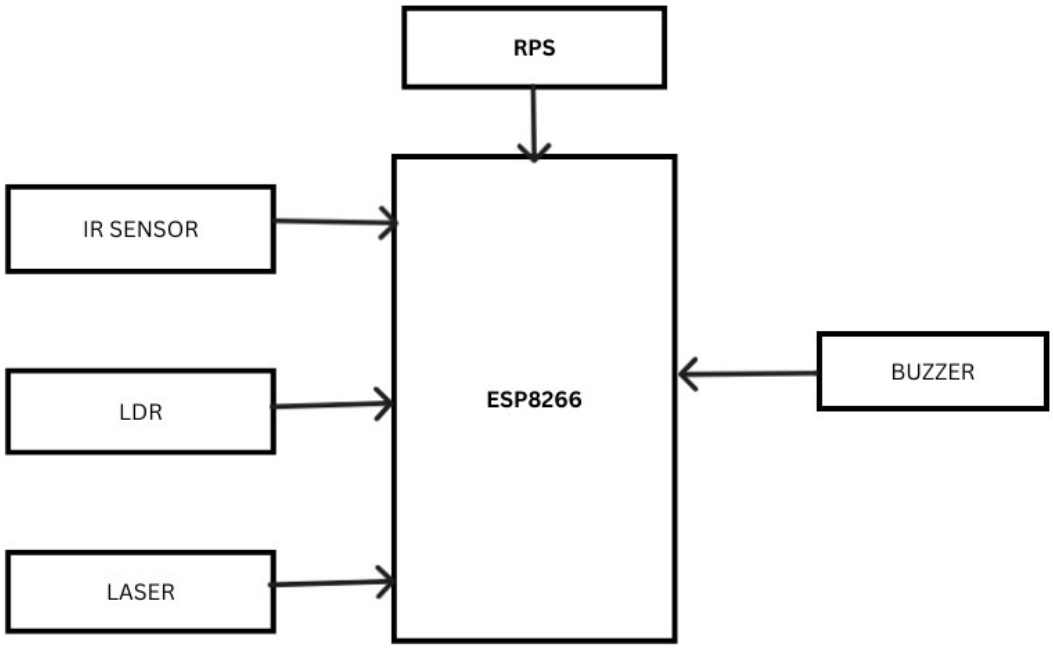
3.2 Objectives

Here are the primary objectives of a bank security system:

1. Asset Protection: Safeguard cash, valuables, and sensitive documents from theft or damage.
2. Prevent Fraud: Deter and detect fraudulent activities, such as identity theft and account manipulation.
3. Customer Safety: Ensure a secure environment for customers to conduct transactions without fear of harm or intimidation.

4. Data Security: Protect sensitive customer information and financial data from cyber threats and unauthorized access.
5. Compliance: Adhere to regulatory requirements and industry standards for security and risk management.
6. Risk Management: Identify, assess, and mitigate potential security risks and vulnerabilities.
7. Incident Response: Quickly respond to and manage security breaches, minimizing impact and downtime.
8. Deterrent: Discourage criminal activity through visible security measures and reputation.
9. Business Continuity: Ensure uninterrupted operations and services despite security incidents or threats.
10. Reputation and Trust: Maintain customer trust and confidence in the bank's ability to protect their assets and information.
By achieving these objectives, a bank security system helps prevent financial losses, reputational damage, and legal liabilities.

3.3 Block Diagram:



3.4 **Tools Required**

Hardware Components

- Node MCU
- IR sensor
- Laser
- Buzzer

Software Components

- ESP8266

Techniques Used

Here are some techniques used in bank security systems:

1. Access Control: Restricting access to authorized personnel and customers.

2. Authentication: Verifying identities through passwords, biometrics, or smart cards.

3. Encryption: Protecting data with algorithms like AES, RSA, and PGP.

4. Intrusion Detection and Prevention (IDPS): Monitoring network traffic for potential threats.

5. Secure Socket Layer/Transport Layer Security (SSL/TLS): Encrypting online transactions.
6. Firewalls: Blocking unauthorized network access.
7. Network Segmentation: Isolating sensitive areas of the network.
8. Surveillance: Monitoring premises with CCTV cameras.
9. Anomaly Detection: Identifying unusual behavior or transactions.
10. Incident Response: Responding to security breaches with pre-defined protocols.
11. Penetration Testing and Vulnerability Assessment: Identifying weaknesses through simulated attacks.
12. Two-Factor Authentication (2FA): Requiring additional verification steps.
13. Fraud Detection: Analyzing transactions for suspicious patterns.
14. Secure Coding Practices: Developing software with security in mind.
15. Regular Security Updates and Patching: Keeping systems up-to-date with latest security fixes.
16. Physical Security: Implementing locks, alarms, and secure storage.

17. Background Checks: Verifying employee and contractor credentials.
18. Training and Awareness: Educating employees on security best practices.
19. Risk Management: Identifying and mitigating potential security risks.
20. Compliance: Adhering to regulatory requirements like GDPR, PCI-DSS, and FFIEC.

These techniques help banks protect their assets, customer data, and reputation from various threats.

WORKING

Here are some additional roles that work together to ensure the security of a bank's security system, with more information on each role:

1. Security Manager:
   - Develops and implements security policies and procedures
   - Conducts risk assessments and vulnerability testing
   - Manages security incidents and response
2. Network Security Engineer:
   - Designs and implements secure network architectures
   - Configures firewalls, VPNs, and intrusion detection systems

- Conducts network vulnerability testing and remediation

3. System Administrator:
   - Installs, configures, and maintains computer systems and software
   - Manages user accounts and access controls
   - Monitors system logs and performance
4. Cybersecurity Analyst:
   - Monitors and analyzes security event logs and threat intelligence
   - Conducts incident response and threat hunting
   - Develops and implements security incident response plans
5. Incident Response Specialist:
   - Responds to security incidents and breaches
   - Conducts forensic analysis and incident containment
   - Develops incident response plans and procedures
6. Access Control Specialist:
   - Manages physical and logical access controls
   - Configures and maintains access control systems
   - Conducts access control audits and compliance checks

7. Surveillance Specialist:
   - Installs, configures, and maintains CCTV and surveillance systems
   - Monitors and reviews surveillance footage
   - Conducts surveillance system maintenance and upgrades
8. Fraud Detection Specialist:
   - Analyzes transactions for suspicious activity
   - Conducts fraud investigations and incident response
   - Develops fraud detection rules and scenarios
9. Penetration Tester:
   - Conducts simulated attacks on computer systems and networks
   - Identifies vulnerabilities and develops remediation plans
   - Conducts penetration testing and vulnerability assessments
10. Security Guard:
    - Provides physical security and access control
    - Responds to security incidents and alarms

- Conducts security patrols and monitoring

These roles work together to ensure the security and integrity of the bank's assets, customer data, and reputation.

ADVANTAGES

A bank security system offers several advantages, including:

1. Protection of Assets: Secure storage and protection of valuable assets, such as cash, jewelry, and important documents.
2. Prevention of Fraud: Detection and prevention of fraudulent activities, like identity theft and account manipulation.
3. Enhanced Customer Safety: Secure environment for customers to conduct transactions without fear of harm or intimidation.
4. Compliance with Regulations: Adherence to industry standards and regulatory requirements, reducing legal and financial risks.
5. Reduced Risk of Burglary and Robbery: Deterrent effect on potential criminals, minimizing the risk of burglary and robbery.
6. Improved Incident Response: Quick response and management of security breaches, minimizing impact and downtime.
7. Enhanced Surveillance: Continuous monitoring and recording of premises, aiding investigations and crime prevention.
8. Access Control: Restricted access to sensitive areas, ensuring only authorized personnel can enter.
9. Data Protection: Encryption and secure storage of sensitive customer information and financial data.
10. Business Continuity: Minimized disruption to banking services, ensuring continuous operation and customer satisfaction.
11. Increased Customer Trust: Demonstration of commitment to security, enhancing customer confidence and loyalty.
12. Reduced Insurance Costs: Lower premiums due to improved security measures.
13. Improved Employee Safety: Secure working environment, reducing stress and anxiety.
14. Enhanced Reputation: Demonstration of commitment to security, enhancing the bank's reputation.

These advantages highlight the importance of a comprehensive bank security system in protecting assets, preventing fraud, and ensuring a safe and secure environment for customers and employees.

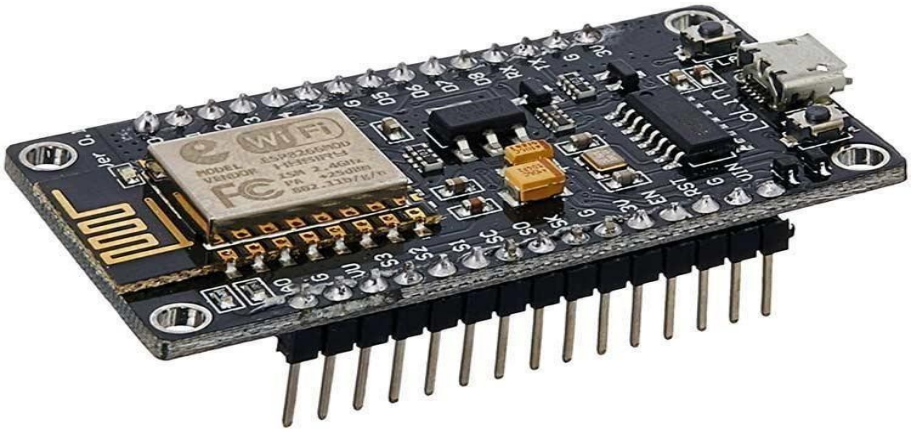
CHAPTER-4

HARDWARE IMPLEMENTATION

4.1Node MCU ESP8266

4.12Description

Node MCU ESP8266 4.1.1 Description Node MCU ESP8266 Description Node MCU is an open-source firmware for which open source prototyping board designs are available. The name “Node MCU” combines “node” and “MCU” (micro-controller unit). The term “Node MCU” strictly speaking refers to the firmware rather than the associated development kits. Both the firmware and prototyping board designs are open source. Node MCU ESP8266 and Node MCU ESP32 are becoming very popular and are almost used in more than 50% IoT based projects today.



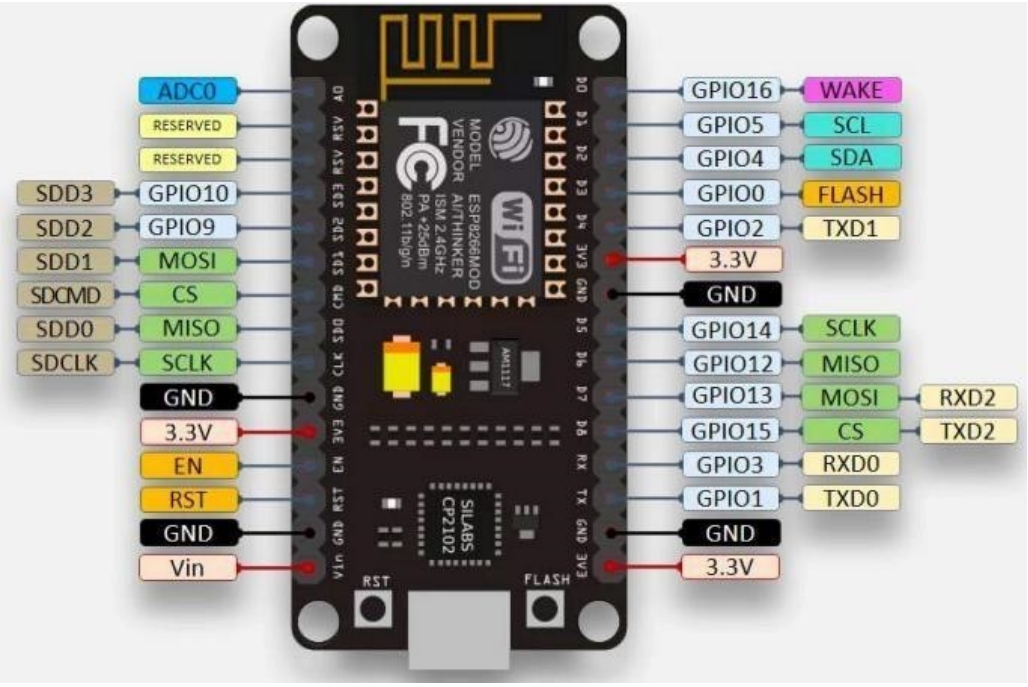
Node MCU

The firmware uses the Lua scripting language. The firmware is based on the eLua project and built on the Espressif Non-OS SDK for ESP8266. It uses many open-source projects, such as luacjson and SPIFFS. Due to resource constraints, users need to select the modules relevant for their project and build a firmware tailored to their needs. Support for the 32-bit ESP32 has also been implemented. The prototyping hardware typically used is a circuit board functioning as a dual in-line package (DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna. The choice of the DIP format allows for easy prototyping on breadboards.

The design was initially was based on the ESP-12 module of the ESP8266, which is a Wi Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications.

About the Node MCU ESP8266 Pinout:

Node MCU ESP8266 Wi-Fi Module is an open-source Lua based firmware and development board specially targeted for IoT based applications. It includes firmware that runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module.



Pin Diagram of Node MCU

4.13 Node MCU ESP8266 Features:

Microcontroller: Tensilica 32-bit RISC CPU Xtensa LX106

Operating Voltage: 3.3V Input

Voltage: 7-12V

Digital I/O Pins (DIO): 16

Analog Input Pins (ADC): 1

UARTs: 1

SPIs: 1

I2Cs: 1 Flash Memory: 4 MB

SRAM: 64 KB

Clock Speed: 80 MHz

USB-TTL based on CP2102 is included onboard, Enabling Plug n Play PCB

Antenna Small Sized module to fit smartly inside your IoT projects

Layout of the Node MCU

4.14 Node MCU ESP8266 Pinout:

For practical purposes ESP8266 Node MCU V2 and V3 boards present identical pinouts. While working on the Node MCU based projects we are interested in the following pins.

Power pins (3.3 V).

Ground pins (GND).

Analog pins (A0).

Digital pins (D0 – D8, SD2, SD3, RX, and TX – GPIO XX)

Most ESP8266 Node MCU boards have one input voltage pin (Vin), three power pins (3.3v), four ground pins (GND), one analog pin (A0), and several digital pins (GPIO XX).

Pin Code Arduino alias

A0 A0 A0

D0 GPIO 16 16

D1 GPIO 5 5

D2 GPIO 4 4

D3 GPIO 0 0

D4 GPIO 2 2

D5 GPIO 14 14

D6 GPIO 12 12

D7 GPIO 13 13

D8 GPIO 15 15SD2 GPIO 9 9

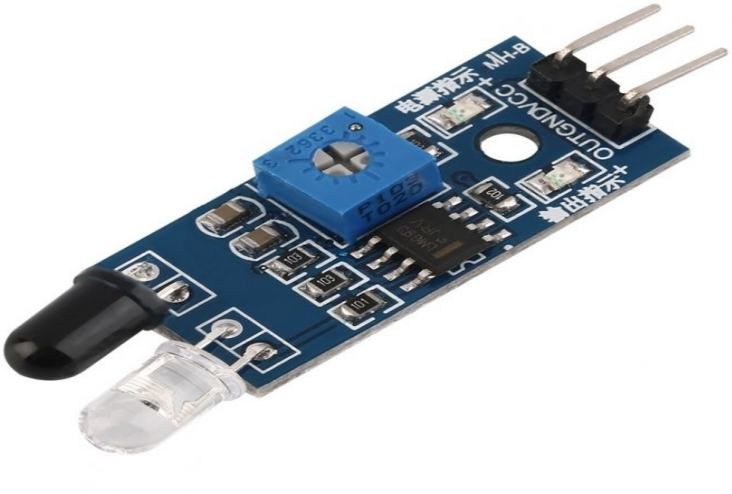
SD3 GPIO 10 10

RX GPIO 3 3

TX GPIO 1 1

4.2 IR SENSOR

IR sensor is an electronic device, that emits the light in order to sense some object of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. Usually, in the, infrared specturm all the objects radiate some form of thermal radiation. These types of radiations are invisible to our eyes, but infrared sensor can detect these radiations.



IR sensor

The emitter is simply an IR LED (Light Emitting Diode) and the detector is simply an IR photodiode . Photodiode is sensitive to IR light of the same wavelength which is emitted by the IR LED. When IR light falls on the photodiode, the resistances and the output voltages will change in proportion to the magnitude of the IR light received.

There are five basic elements used in a typical infrared detection system: an infrared source, a transmission medium, optical component, infrared detectors or receivers and signal processing. Infrared lasers and Infrared LED's of specific wavelength used as infrared sources.

The three main types of media used for infrared transmission are vacuum, atmosphere and optical fibers. Optical components are used to focus the infrared radiation or to limit the spectral response.

4.2.1 Types of IR Sensor

There are two types of IR sensors are available and they are,

- Active Infrared Sensor
- Passive Infrared Sensor

Active Infrared Sensor

Active infrared sensors consist of two elements: infrared source and infrared detector. Infrared sources include the LED or infrared laser diode. Infrared detectors include photodiodes or phototransistors. The energy emitted by the infrared source is reflected by an object and falls on the infrared detector.

Passive Infrared Sensor

Passive infrared sensors are basically Infrared detectors. Passive infrared sensors do not use any infrared source and detector. They are of two types: quantum and thermal. Thermal infrared sensors use infrared energy as the source of heat. Thermocouples, pyroelectric detectors and bolometers are the common types of thermal infrared detectors. Quantum type infrared sensors offer higher detection performance. It is faster than thermal type infrared detectors. The photo sensitivity of quantum type detectors is wavelength dependent.

IR Sensor Working Principle

There are different types of infrared transmitters depending on their wavelengths, output power and response time. An IR sensor consists of an IR LED and an IR Photodiode, together they are called as PhotoCoupler or OptoCoupler.

4.2.2 IR Transmitter or IR LED

Infrared Transmitter is a light emitting diode (LED) which emits infrared radiations called as IR LED's. Even though an IR LED looks like a normal LED, the radiation emitted by it is invisible to the human eye.

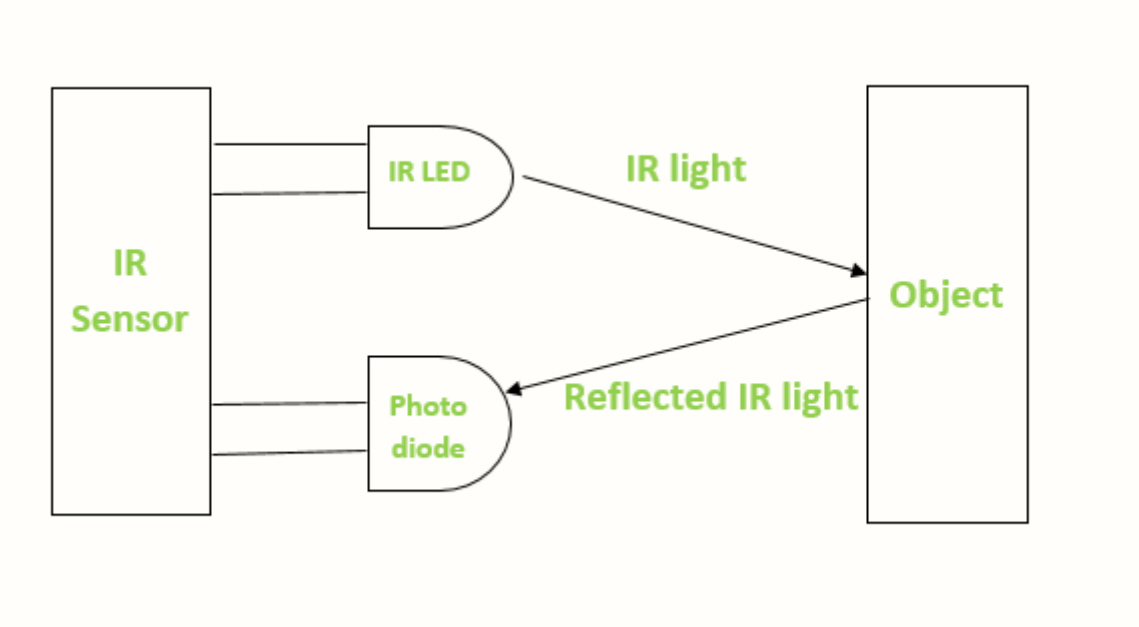
The picture of an Infrared LED is shown below.

4.2.3 IR Receiver or Photodiode

Infrared receivers or infrared sensors detect the radiation from an IR transmitter. IR receivers come in the form of photodiodes and phototransistors. Infrared Photodiodes are different from normal photo diodes as they detect only infrared radiation. Below image shows the picture of an IR receiver or a photodiode,

Different types of IR receivers exist based on the wavelength, voltage, package, etc. When used in an infrared transmitter – receiver combination, the wavelength of the receiver should match with that of the transmitter.

The emitter is an IR LED and the detector is an IR photodiode. The IR photodiode is sensitive to the IR light emitted by an IR LED. The photo-diode's resistance and output voltage change in proportion to the IR light received. This is the underlying working principle of the IR sensor.

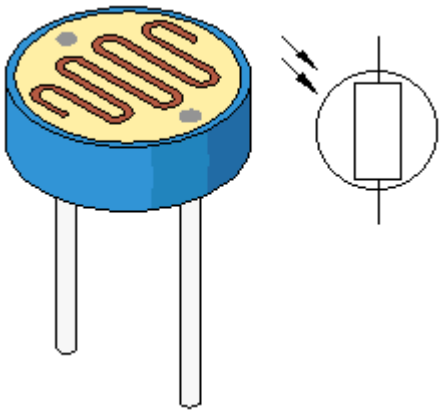


When the IR transmitter emits radiation, it reaches the object and some of the radiation reflects back to the IR receiver. Based on the intensity of the reception by the IR receiver, the output of the sensor defines.

4.4 LDR(LIGHT DEPENDENT RESISTOR)

LDR (Light Dependent Resistor) as the name states is a special type of resistor that works on the photoconductivity principle means that resistance changes according to the intensity of light. Its resistance decreases with an increase in the intensity of light.

It is often used as a light sensor, light meter, Automatic street light, and in areas where we need to have light sensitivity. LDR is also known as a Light Sensor. LDR are usually available in 5mm, 8mm, 12mm, and 25mm dimensions.



4.4.1LDR Working Principle

It works on the principle of photoconductivity whenever the light falls on its photoconductive material, it absorbs its energy and the electrons of that photoconductive material in the valence band get excited and go to the conduction band and thus increasing the conductivity as per the increase in light intensity.

Also, the energy in incident light should be greater than the bandgap gap energy so that the electrons from the valence band got excited and go to the conduction band.

The LDR has the highest resistance in dark around 1012 Ohm and this resistance decreases with the increase in Light.

4.4.2 Applications:

Photo resistors come in many different types. Inexpensive cadmium sulfide cells can be found in many consumer items such as camera light meters, clock radios, security alarms, street lights and outdoor clocks.
They are also used in some dynamic compressors together with a small incandescent lamp or light emitting diode to control gain reduction.
Lead sulfide and indium antimonite LDRs are used for the mid infrared spectral region. Ge:Cu photoconductors are among the best far-infrared detectors available, and are used for infrared astronomy and infrared spectroscopy.

4.5 BUZZER

An audio signaling device like a beeper or buzzer may be electromechanical or piezoelectric or mechanical type. The main function of this is to convert the signal from audio to sound. Generally, it is powered through DC voltage and used in timers, alarm devices, printers, alarms, computers, etc. Based on the various designs, it can generate different sounds like alarm, music, bell & siren
.

The pin configuration of the buzzer is shown above. It includes two pins namely positive and negative. The positive terminal of this is represented with the '+' symbol or a longer terminal. This terminal is powered through 6Volts whereas the negative terminal is represented with the '-'symbol or short terminal and it is connected to the GND terminal.

4.5.1 Specifications

The specifications of the buzzer include the following.

- Color is black
- The frequency range is 3,300Hz
- Operating Temperature ranges from – 20° C to +60°C
- Operating voltage ranges from 3V to 24V DC
- The sound pressure level is 85dBA or 10cm
- The supply current is below 15mA

4.5.2 **Working Principle**

The working principle of a buzzer depends on the theory that, once the voltage is given across a piezoelectric material, then a pressure difference is produced. A piezo type includes piezo crystals among two conductors.

Once a potential disparity is given across these crystals, then they thrust one conductor & drag the additional conductor through their internal property. So this continuous action will produce a sharp sound signal.

CHAPTER-5

SOFTWARE IMPLENTATION

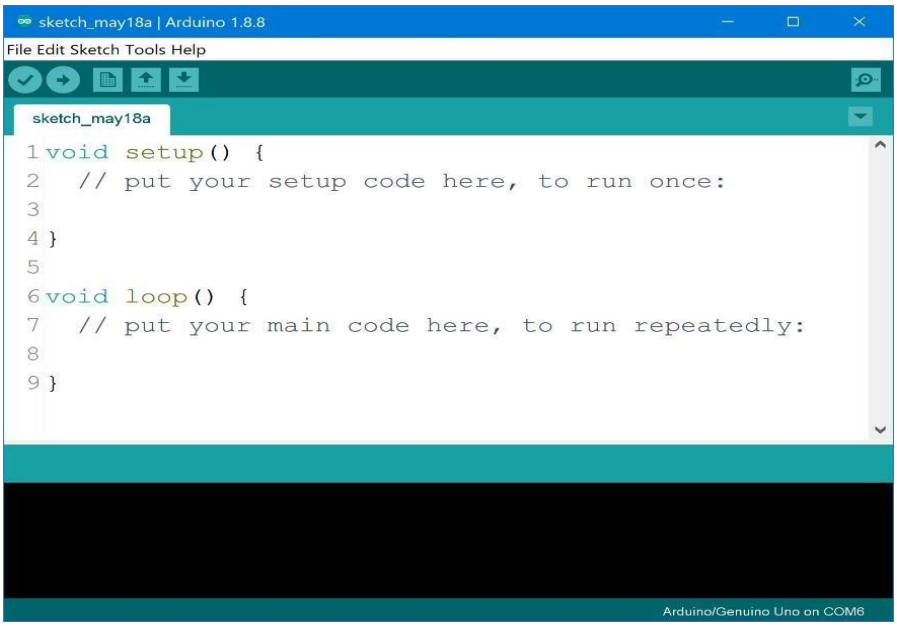
5.1 Arduino IDE

5.1.1 Introduction to Arduino IDE

IDE stands for Integrated Development Environment - An official software introduced by Arduino.cc that is mainly used for writing, compiling and uploading the code in almost all Arduino modules/boards. Arduino IDE is open-source software and is easily available to download & install from Arduino Official Site.

In this post, I'll take you through the brief Introduction of the Software, how you can install it, and make it ready for your required Arduino module.

Let's dive in and get down to the nitty-gritty of this Software.



Arduino IDE is an open-source software, designed by Arduino.cc and mainly used for writing, compiling & uploading code to almost all Arduino Modules.

It is an official Arduino software, making code compilation too easy that even a common person with no prior technical knowledge can get their feet wet with the learning process.It is available for all operating systems i.e., MAC, Windows, Linux and runs on the Java Platform that comes with inbuilt functions and commands that play a vital role in debugging, editing and compiling the code.A range of Arduino modules available including Arduino Uno, Arduino Mega, Arduino Leonardo, Arduino Micro and many more.Each of them contains a microcontroller on the board that is actually programmed and accepts the information in the form of code.The main code, also known as a sketch, created on the IDE platform will ultimately generate a Hex File which is then transferred and uploaded in the controller on the board.The IDE environment mainly contains two basic parts: Editor and Compiler where former is used for writing the required code and later is used for compiling and uploading the code into the given Arduino Module.

This environment supports both C and C++ languages.

5.1.2 How to Download Arduino IDE

You can download the Software from Arduino main website. As I said earlier, the software is available for common operating systems like Linux, Windows, and MAX, so make sure you are downloading the correct software version that is easily compatible with your operating system.

8.1 or Windows 10, as the app version is not compatible with Windows 7 or older version of this operating system.

You can download the latest version of Arduino IDE for Windows (Non admin standalone version), by clicking below button:

5.1.2 Arduino IDE Download

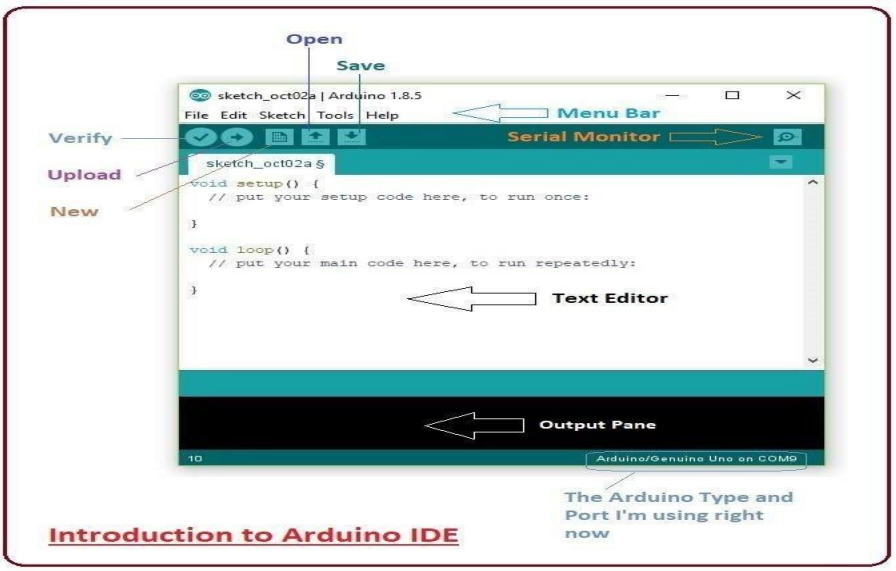
The IDE environment is mainly distributed into three sections.

1.Menu Bar

2.Text Editor

3.Output Pane

As you download and open the IDE software, it will appear like an image below:



Introduction to Arduino IDE

The bar appearing on top is called Menu Bar that comes with five different options as

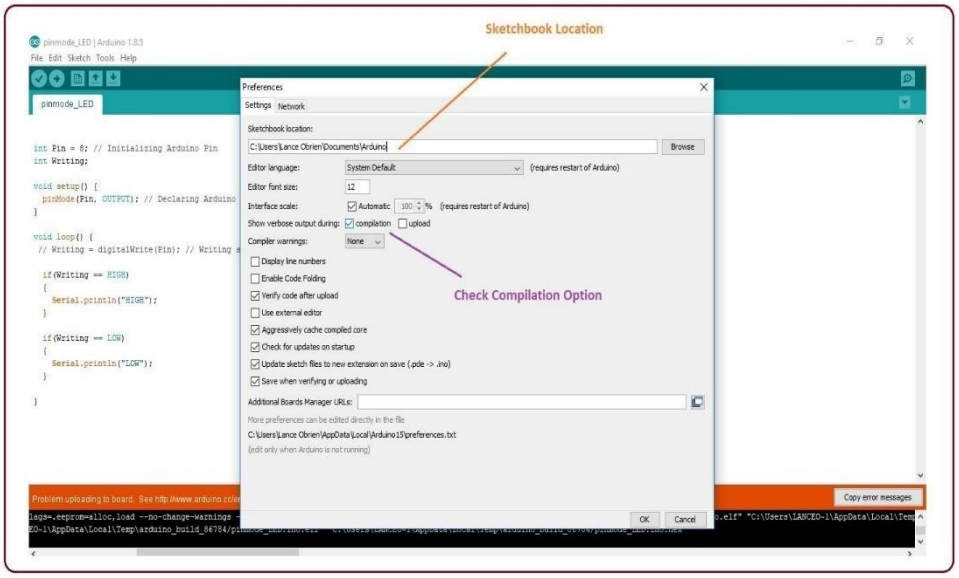
- File - You can open a new window for writing the code or open an existing one.

The following table shows number of further subdivisions the file option is categorized into:

File	
New	This is used to open new text editor window to write your code
Open	Used for opening the existing written code
Open Recent	The option reserved for opening recently closed program
Sketchbook	It stores the list of codes you have written for your project
Examples	Default examples already stored in the IDE software
Close	Used for closing the main screen window of recent tab. If two tabs are open, it will ask you again as you aim to close the second tab
Save	It is used for saving the recent program
Save as	It will allow you to save the recent program in your desired folder
Page setup	Page setup is used for modifying the page with portrait and landscape options. Some default page options are already given from which you can select the page you intend to work on
Print	It is used for printing purpose and will send the command to the printer
Preferences	It is page with number of preferences you aim to setup for your text editor page
Quit	It will quit the whole software all at once

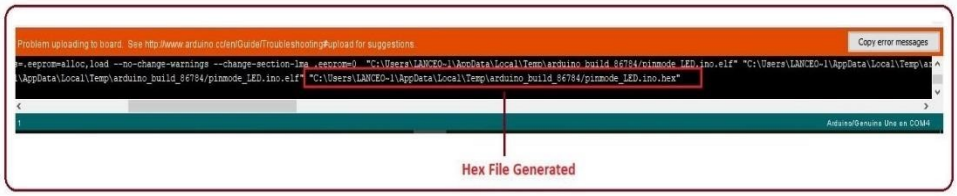
File subdivisions in Arduino IDE

As you go to the preference section and check the compilation section, the Output Pane will show the code compilation as you click the upload button.



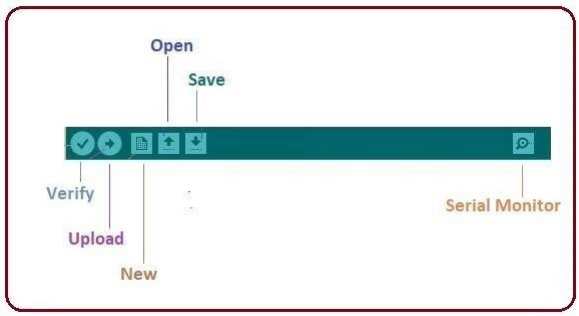
Selection of compilation

And at the end of the compilation, it will show you the hex file it has generated for the recent sketch that will send to the Arduino Board for the specific task you aim to achieve



Hex file generation

- Sketch - For compiling and programming
- Tools - Mainly used for testing projects. The Programmer section in this panel is used for burning a boot loader to the new microcontroller.
- Help - In case you are feeling Edit - Used for copying and pasting the code with further modification for font
- sceptical about software, complete help is available from getting started to troubleshooting.
- The Six Buttons appearing under the Menu tab are connected with the running program as follows

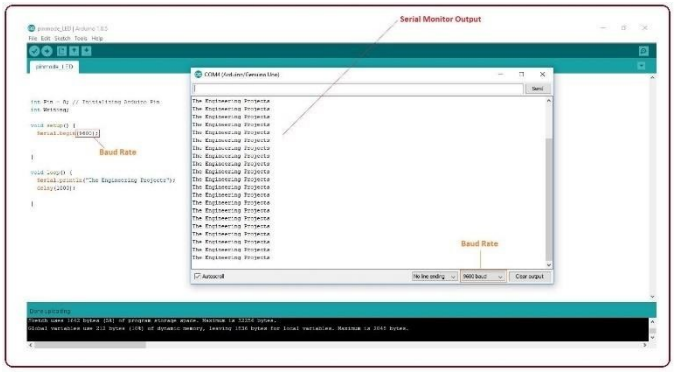


Serial monitor

- The check mark appearing in the circular button is used to verify the code. Click this once you have written your code.
- The arrow key will upload and transfer the required code to the Arduino board.
- The dotted paper is used for creating a new file.
- The upward arrow is reserved for opening an existing Arduino project.
- The downward arrow is used to save the current running code.
- The button appearing on the top right corner is a Serial Monitor - A separate pop-up window that acts as an independent terminal and plays a vital role in

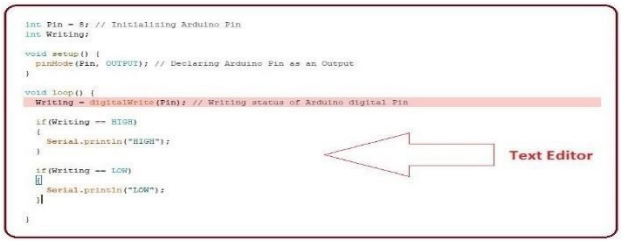
sending and receiving the Serial Data. You can also go to the Tools panel and select Serial Monitor, or pressing Ctrl+Shift+M all at once will open it instantly. The Serial Monitor will actually help to debug the written Sketches where you can get a hold of how your program is operating. Your Arduino Module should be connected to your computer by USB cable in order to activate the Serial Monitor.

- You need to select the baud rate of the Arduino Board you are using right now. For my Arduino Uno Baud Rate is 9600, Monitor, the output will show as the image below.



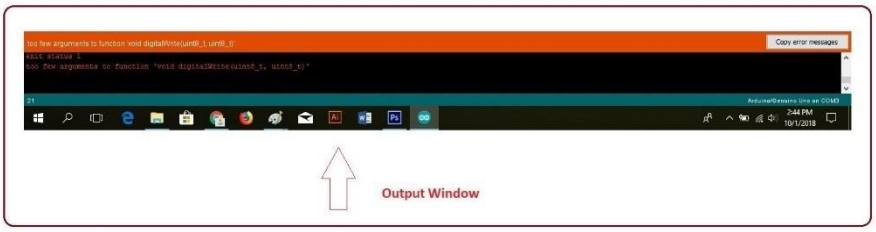
output of the serial monitor

The main screen below the Menu bard is known as a simple text editor used for writing the required code



Text editor

Output Pane that mainly highlights the compilation status of the running code: the memory used by the code, and errors that occurred in the program. You need to fix the bottom of the main screen is described as those errors before you intend to upload the hex file into your Arduino Module.



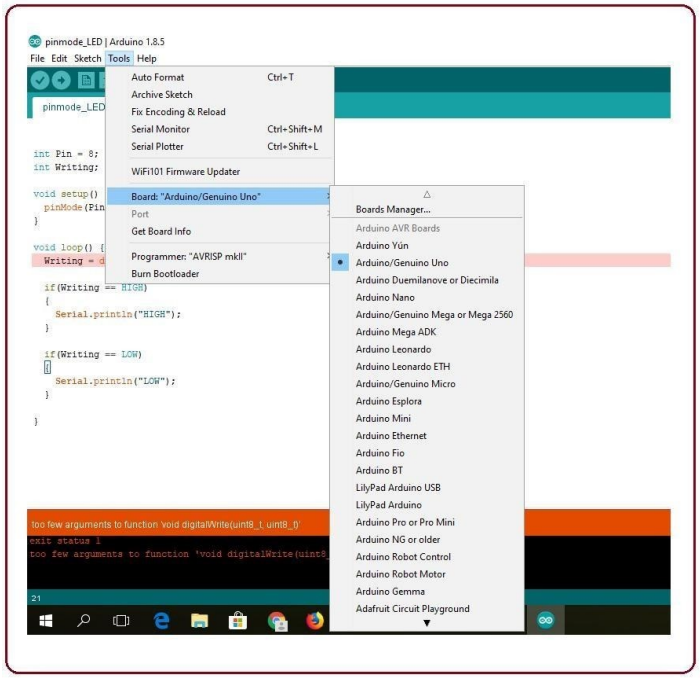
output window

More or less, Arduino C language works similar to the regular C language used for any embedded system microcontroller, however, there are some dedicated libraries used for calling and executing specific functions on the board.

5.1.3 Libraries

- Libraries are very useful for adding extra functionality into the Arduino Module.
- There is a list of libraries you can check by clicking the Sketch button in the menu bar and going to Include Library.
- As you click the Include Library and Add the respective library it will be on the top of the sketch with a #include sign. Suppose, I Include the Liquid Crystal library, it will appear on the text editor as

#include <Liquid Crystal. h>



Selection of tools

- As you click the Include Library and Add the respective library it will be on the top of the sketch with a #include sign. Suppose, I Include the Liquid Crystal library, it will appear on the text editor as

  #include <Liquid Crystal.h>

Most of the libraries are preinstalled and come with the Arduino software

However, you can also download them from external sources.

5.1.4 Making Pins Input or Output.

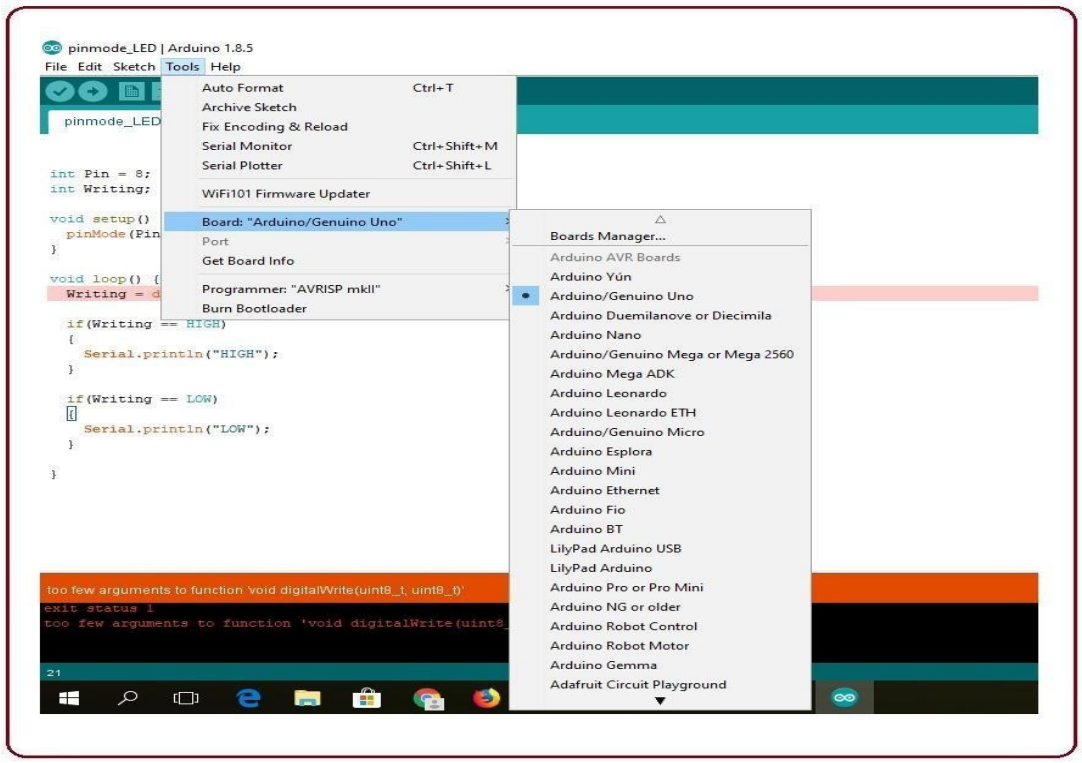
The digitalRead and digitalWrite commands are used for addressing and making the Arduino pins as an input and output respectively. These commands are text sensitive i.e., you need to write them down the exact way they are given like digitalWrite starting with small "d" and write with capital "W". Writing it down with DigitalWrite or digitalWrite won't be calling or addressing any function.

Making Pins Input or Output

The digitalRead and digitalWrite commands are used for addressing and making the Arduino pins as an input and output respectively. These commands are text sensitive i.e., you need to write them down the exact way they are given like digitalWrite starting with small "d" and write with capital "W". Writing it down with DigitalWrite or digitalWrite won't be calling or addressing any function.

5.4.5 How to Select the Board

- In order to upload the sketch, you need to select the relevant board you are using and the ports for that operating system.
- As you click the Tools on the menu, it will open like the figure below:



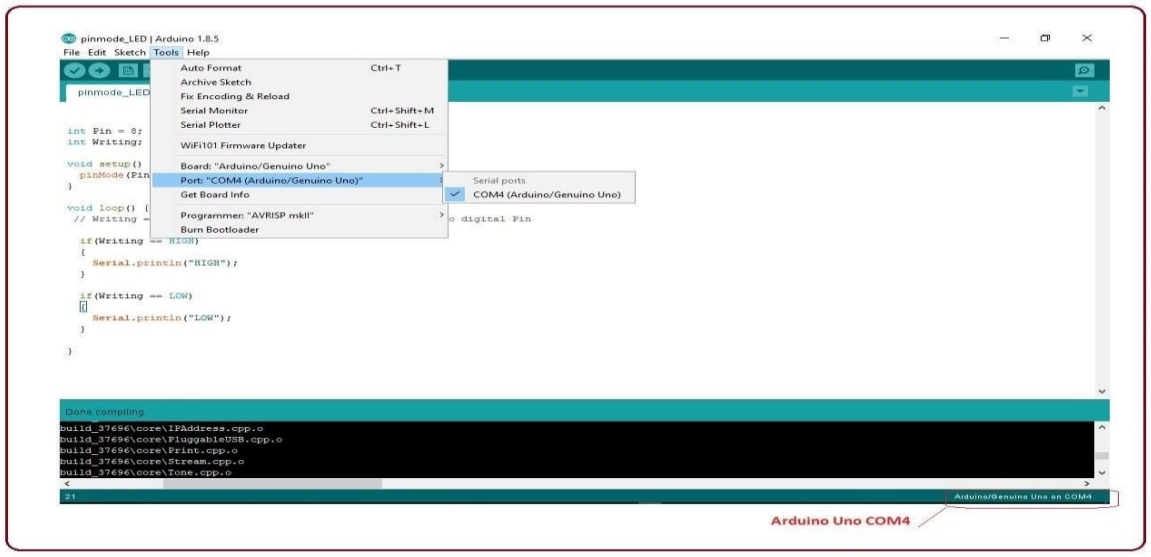
Selection of board manager

- Just go to the "Board" section and select the board you aim to work on. Similarly, COM1, COM2, COM4, COM5, COM7 or higher are reserved for the

serial and USB board. You can look for the USB serial device in the port section of the Windows Device Manager.

- The following figure shows the COM4 that I have used for my project, indicating the Arduino Uno with the COM4 port at the right bottom corner of the screen.

- After correct selection of both Board and Serial Port, click the verify and then upload button appearing in the upper left corner of the six-button section or you can go to the Sketch section and press verify/compile and then upload.
- The sketch is written in the text editor and is then saved with the file extension into. It is important to note that the recent Arduino Modules will reset automatically as you compile and press the upload button the IDE software, however, the older versions may require the physical reset on the board.
- Once you upload the code, TX and RX LEDs will blink on the board, indicating the desired program is running successfully.



Selection of port

Note: The port selection criteria mentioned above are dedicated to Windows operating system only, you can check this Guide if you are using MAC or Linux.

The amazing thing about this software is that no prior arrangement or bulk of the mess is required to install this software, you will be writing your first program within 2 minutes after the installation of the IDE environment.

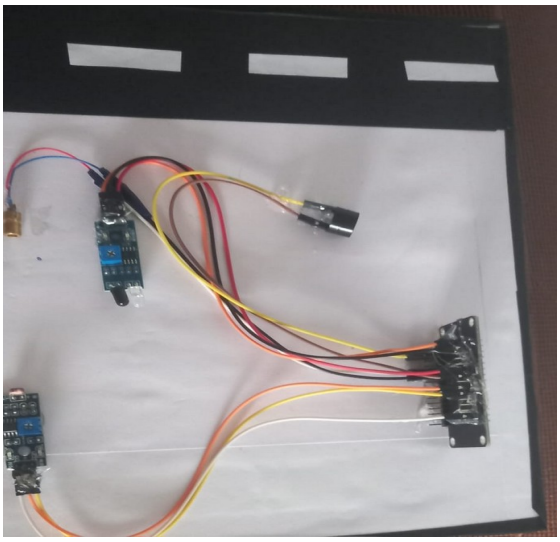
5.1.6 Uploading

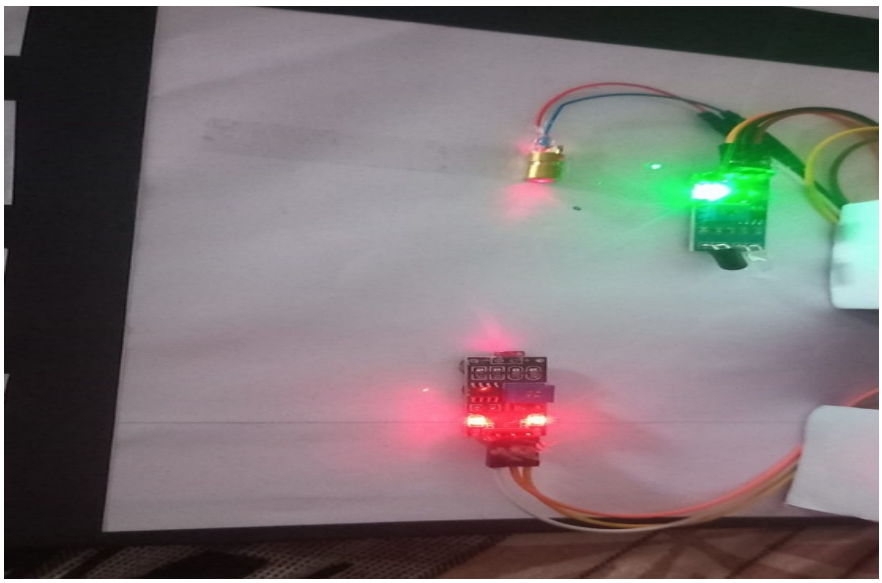
After writing your code, click on the upload button which is above the window and the code will be directly uploaded into the Node MCU with a cable wire connector.

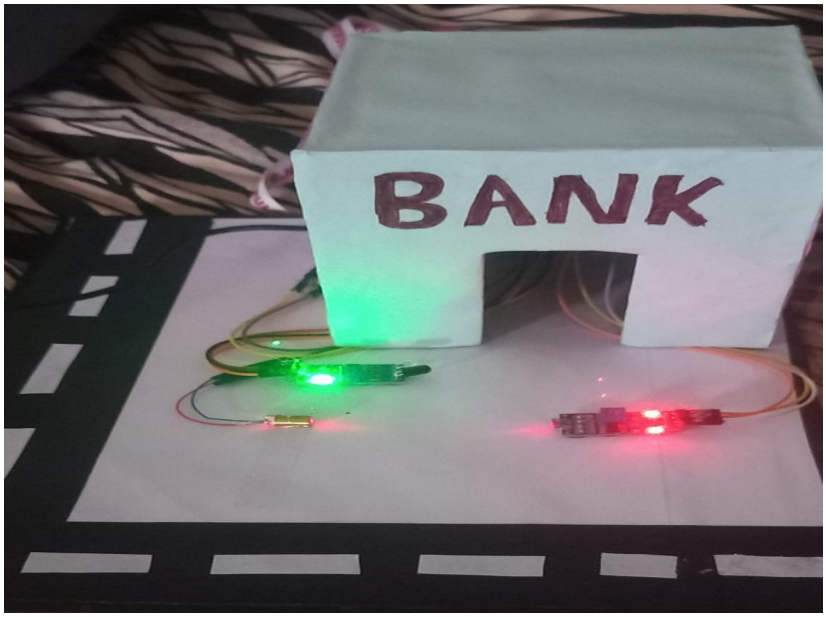
CHAPTER-6

RESULT

When the laser beam falling over the LDR is interrupted by the object in the field of laser net, hence the LDR develops an output voltage and the alarm rings showing the sign of any intruders. The Laser Security System has been successfully designed and developed. The buzzer is turned on as the laser beam falling on the LDR is interrupted. The experimental model was made according to the block diagram and the result was as expected.







IR sensor also detects if any intruders come in between plays the buzzer sound these helps us in more security if there is any failure in laser.

CONCLUSION

Laser Security system provides us the security against any crime, theft in banks it also helps in our day-to-day life. Various electronic security systems can be used at home and other important working places for security and safety purposes. It is a great opportunity ad source of saving man power contributing no wastage of electricity. The “Laser Security System” is an important helping system. Using this system robbery, thefts, & crime can be avoided to large extend. Avoiding thieves results in the safety of our financial assets and thereby this system provides us protection against all.

The IR sensor in this project also helps in protects which senses an object which even helps us even if the thief escapes from the laser.IR sensor helps us to detect the object and plays the buzzer sound which alerts people around the bank. The Laser & LDR system is highly sensitive with a great range of working. The system senses the light emitted by the Laser falling over the LDR connected with the circuit. IR sensor, Laser protects bank from theft or any another illegal activity.

SOURCE CODE

```
define TS_ENABLE_SSL // For HTTPS SSL connection

#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include "secrets.h"
#include "ThingSpeak.h" // always include thingspeak header file after other header files and custom macros

char ssid[] ="AIML BATCH 6";   // your network SSID (name)
char pass[] = "AIMLAIML";   // your network password
int keyIndex = 0;            // your network key Index number (needed only for WEP)
WiFiClientSecure  client;

unsigned long myChannelNumber =2597333;
const char * myWriteAPIKey = "EZBBC719W1W1WLB47";

// Initialize our values
int ir;
int ldr;
int buzzer;
int number4 = random(0,100);
String myStatus = "";

// Fingerprint check, make sure that the certificate has not expired.
const char * fingerprint = NULL; // use SECRET_SHA1_FINGERPRINT for fingerprint check

void setup() {
  pinMode(ir,INPUT);
```

```
 pinMode(ldr,INPUT);
 pinMode(buzzer,OUTPUT);
 Serial.begin(115200);  // Initialize serial
 while (!Serial) {
  ; // wait for serial port to connect. Needed for Leonardo native USB port only
 }

 WiFi.mode(WIFI_STA);

 if(fingerprint!=NULL){
  client.setFingerprint(fingerprint);
 }
 else{
  client.setInsecure(); // To perform a simple SSL Encryption
 }

 ThingSpeak.begin(client);  // Initialize ThingSpeak
}

void loop() {
 int ldrstatus=digitalRead(ldr);
 Serial.println(ldrstatus);
 int a=digitalRead(ir);
 if(a==0 || ldrstatus==1)
 {
  digitalWrite(buzzer,HIGH);
 }
 else
 {
  digitalWrite(buzzer,LOW);
 }
 // Connect or reconnect to WiFi
 if(WiFi.status() != WL_CONNECTED){
  Serial.print("Attempting to connect to SSID: ");
```

```
  Serial.println(SECRET_SSID);
  while(WiFi.status() != WL_CONNECTED){
   WiFi.begin(ssid, pass);  // Connect to WPA/WPA2 network. Change this line
if using open or WEP network
    Serial.print(".");
    delay(5000);
  }
  Serial.println("\nConnected.");
 }

 // set the fields with the values
 ThingSpeak.setField(1, ir);
 ThingSpeak.setField(2, ldr);
 ThingSpeak.setField(3, buzzer);
 ThingSpeak.setField(4, number4);

 // figure out the status message
 if(ir > ldr){
  myStatus = String("field1 is greater than field2");
 }
 else if(ir < ldr){
  myStatus = String("field1 is less than field2");
 }
 else{
  myStatus = String("field1 equals field2");
 }

 // set the status
 ThingSpeak.setStatus(myStatus);

 // write to the ThingSpeak channel
 int x = ThingSpeak.writeFields(myChannelNumber, myWriteAPIKey);
 if(x == 200){
  Serial.println("Channel update successful.");
```

```
  }
  else{
    Serial.println("Problem updating channel. HTTP error code " + String(x));
  }

  // change the values
  ir++;
  if(ir > 99){
    ir = 0;
  }
  ldr = random(0,100);
  buzzer = random(0,100);
  number4 = random(0,100);

  delay(20000); // Wait 20 seconds to update the channel again
}
```

REFERENCES

1. https://ijcrt.org/papers/IJCRT2304139.pdf
2. https://projectsfactory.in/product/bank-locker-security-system-with-password-and-intruder-alarm/
3. https://www.electronicshub.org/laser-security-system/
4. https://www.securicoelectronics.com/solutions/bfsis/
5. https://www.myprojectcircuits.com/project-category/medical-laboratory-science-project-topics/
6. https://www.slideshare.net/slideshow/i03014853/44337698
7. https://www.myprojectcircuits.com/materials/design-and-construction-of-a-ir-sensor-based-security-system/
8. https://projectsfactory.in/product/bank-locker-security-system-with-password-and-intruder-alarm/

INTERNSHIP COMPLETION CERTIFICATE

PROUDLY PRESENTED TO:

Chennamsetty Anitha

Student of Vignan's Nirula Institute of Technology and Science for Women,
Reg No: 22NN1A4208 has successfully completed an
Internship on IOT Internship (13-05-2024 to 06-07-2024)
program at Vijayawada. During her internship program with us, She was found punctual, hardworking and inquisitive.

This certificate was awarded by:

Md. Mobina

MOBINA MD

Managing Director

06-07-2024

Issue Date

INTERNSHIP COMPLETION CERTIFICATE


AICTE
APSCHE
ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION
INTERNSHIP COMPLETION


AICTE
APSCHE
ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION
INTERNSHIP COMPLETION