KARNATAK LAW SOCIETY'S

GOGTE INSTITUTE OF TECHNOLOGY

UDYAMBAG, BELAGAVI-590008

(An Autonomous Institution under Visvesvaraya Technological University Belagavi)

(APPROVED BY AICTE, NEW DELHI)

A Report of **Principles Of Communication Systems(21EC44)** *Course Activity On*

Communication setup for security system

Submitted in partial fulfillment of the requirement for the award of the degree of

Bachelor of Engineering
In
Electronics and Communication

Submitted By

Shreyas Arjunwadkar (2GI21EC131)

GUIDED BY

Prof.G.P.Kadam

KARNATAK LAW SOCIETY'S

GOGTE INSTITUTE OF TECHNOLOGY

UDYAMBAG, BELAGAVI-590008

(An Autonomous Institution under Visvesvaraya Technological University Belagavi)

(APPROVED BY AICTE, NEW DELHI)

Department of Electronics and Communication

CERTIFICATE

This is to certify that the course activity entitled "Communication setup for security system" is a bona-fide record of the course activity work done by **Yash Betageri(2GI21EC182),TanviHunakunti(2GI21EC156),ShreyasArjunwadkar(2GI21EC131)SiddhuSingadi(2GI21EC141**),under my supervision and guidance, in partial fulfillment of the requirements for the Outcome Based Education Paradigm in Communication from Googte Institute of Technology for the academic year **2022-2023.**

It is certified that all corrections/suggestions indicated have been incorporated in the report. The course project report has been approved as it satisfies the academic requirement prescribed for the said degree.

GUIDED BY **HOD**

Prof.G.P.Kadam

ABSTRACT

This project focuses on designing and implementing a communication setup for a security system that utilizes an ultrasonic sensor, a Wi-Fi module, and an RFID tag, controlled through a mobile phone. The objective is to create a reliable and efficient security system with enhanced access control and monitoring capabilities.

The communication setup comprises a combination of innovative technologies. The ultrasonic sensor acts as a detection mechanism, identifying the presence of objects or individuals within a specific range and triggering an alert signal to the mobile phone. The Wi-Fi module provides wireless connectivity, enabling seamless data transmission between the security system and the mobile phone. The RFID tag serves as a contactless identification method, allowing authorized users to interact with the system by simply waving their mobile phone.

The mobile phone acts as the central control unit, receiving signals from the ultrasonic sensor and sending commands to the Wi-Fi module. Based on the received data and instructions, the system can activate alarms, send notifications, or grant/deny access to individuals based on the verification of their RFID tags.

This project offers advantages over traditional security systems by introducing ‘ 54reliable detection through the ultrasonic sensor, convenient wireless communication via the Wi-Fi module, and efficient access control using RFID tags. The integration and coordination of these components provide a comprehensive and user-friendly security solution for both residential and commercial applications.

Overall, the proposed communication setup for the security system aims to deliver effective monitoring and access control capabilities, leveraging the technologies of ultrasonic sensors, Wi-Fi modules, RFID tags, and mobile phones.

INDEX

1. INTRODUCTION

In today's fast-paced world, security is of paramount concern for both individuals and organizations. With
advancements in technology, there is now a growing demand for innovative security systems that offer reliable and convenient methods of access control and monitoring. This project aims to develop a communication setup for a security system that combines the use of an ultrasonic sensor, a Wi-Fi module, and an RFID tag, all coordinated through a mobile phone.

The core components of this system involve an ultrasonic sensor, which helps in detecting obstacles or intrusions within a specific range, a Wi-Fi module allowing wireless connectivity for data transmission, and a RFID tag which enables contactless identification and authentication. The mobile phone acts as a central device that receives the sensor data and controls the security system remotely.

This project offers several benefits over traditional security systems. First, the use of an ultrasonic sensor provides an extra layer of security by detecting and alerting in real-time for any unauthorized activities or obstacles. Second, the integration of a Wi-Fi module allows for convenient wireless communication and control, eliminating the need for complex wiring installations. Third, the utilization of an RFID tag offers a contactless and efficient method of identification, enhancing user experience and eliminating the need for physical keys or cards.

2. COMPONENTS USED

1. Ultrasonic Sensor:

An ultrasonic sensor is a device that uses sound waves at frequencies higher than the human hearing range to detect objects and measure distances. In a security system, an ultrasonic sensor can be used to detect movement or proximity of objects within its range.

2. RFID Tag:

RFID (Radio Frequency Identification) tags are small electronic devices that store and transmit data wirelessly using radio frequencies. These tags consist of an integrated circuit and an antenna, and they can be attached to objects or individuals for identification and tracking purposes. In a security system, RFID tags can be used for access control or to identify authorized individuals or objects.

3. Mobile Phone:

A mobile phone can serve as a central control or monitoring device for the security system. By connecting to the system through Wi-Fi, the mobile phone can receive real-time notifications, control system parameters, and interact with other components such as RFID tags.

4. ESP8266 Wi-Fi Module:

The ESP8266 is a versatile and cost-effective Wi-Fi module capable of establishing wireless communication with other devices. It enables the security system to transmit data, such as detection events or access requests, to a central monitoring unit via a Wi-Fi network.

3. OBJECTIVE AND PROBLEM STATEMENT

- Distance-based Security Activation
- System Design and Integration
- RFID-based Authentication
- Real-time Notifications
- Remote Monitoring and Control
- Data Logging and Analysis
- Security and Privacy Considerations
- System Testing and Validation
- Scalability and Future Expansion

PROBLEM STATEMENT:

In today's world, security is of utmost importance, be it in residential buildings, offices, or public spaces. To ensure the safety and protection of these areas, advanced security systems are necessary. This project aims to develop a communication setup for a security system that utilizes an ultrasonic sensor, RFID (Radio Frequency Identification) tags, and an ESP8266 module.

Develop an efficient communication setup for a security system that uses an ultrasonic sensor, RFID tags, and the ESP8266 module. The system should be able to detect the presence of unauthorized individuals in a designated area and provide real-time alerts to the user on the mobile phone.

4. DESIGN AND IMPLEMENTATION

1. Initial Setup: Configure the ESP8266 WiFi module to connect to your local wireless network. This involves providing the necessary credentials (e.g., SSID and password) to the module. Once connected, the module will have access to the local network and the internet.

2. Ultrasonic Sensor Integration: Connect the ultrasonic sensor to the ESP8266 module. Whenever the sensor detects an object within the specified range, it triggers the ESP8266 to perform an action. For example, it could send a signal to the mobile phone application indicating that motion has been detected.

3. RFID Tag Integration: Connect an RFID reader to the ESP8266 module. When an RFID tag comes within range of the reader, it reads the tag's unique identifier. The ESP8266 can then send this information to the mobile phone application, which can validate the tag and determine if the user is authorized or not.

4. Mobile Phone Application: Develop a mobile phone application that communicates with the ESP8266 module over the WiFi network. The application should be capable of receiving data from the security system, such as notifications when motion is detected or when an RFID tag is read. It should also allow the user to send commands to the security system, such as arming or disarming the system.

5. Security System Control: Based on the data received from the ultrasonic sensor and RFID reader, the mobile phone application can control the security system. For example, if an unauthorized RFID tag is detected, the application can trigger an alarm or send a notification to the user. Similarly, the user can use the application to arm or disarm the security system remotely.

By integrating these components and establishing the communication setup, you can create a security system that utilizes ultrasonic sensing, RFID technology, and mobile phone control to enhance security and provide remote monitoring capabilities.

5. RESULT AND ANALYSIS

The result and analysis of the project would depend on the specific implementation and requirements of the system. However, here are some potential results and analysis that can be derived from the project:

1. Object Detection: The ultrasonic sensor would provide the ability to detect objects within a certain range. The result would be the distance measurements or presence detection of objects. The analysis can involve tracking the movement patterns of objects or individuals within the monitored area.

2. RFID Tag Detection: When an RFID tag is brought close to the RFID reader, the system would identify the unique identifier associated with the tag. The result would be the detection of authorized or unauthorized tags. The analysis can involve logging the presence and movement of authorized tags or triggering alarms and notifications for unauthorized tags.

3. Mobile Phone Control: With the mobile phone application, users can remotely control the security system, such as arming or disarming it. The result would be the successful transmission of commands from the mobile phone to the security system. The analysis can involve monitoring the usage patterns and activities performed through the mobile application.

4. Security Notifications: The system can send notifications to the mobile phone application based on detected events, such as motion detection or unauthorized tag detection. The result would be the successful delivery of

notifications to the user. The analysis can involve tracking the frequency and types of notifications received to identify any unusual or suspicious activities.

5. System Reliability: The analysis can focus on the overall reliability and stability of the communication setup. It can involve monitoring the connection between the ESP8266 WiFi module and the local network, ensuring consistent data transmission, and addressing any potential issues or failures in the system.

6. User Experience: The analysis can assess the usability and user experience of the mobile phone application. It can involve gathering user feedback on the ease of use, intuitiveness of controls, and overall satisfaction with the system's functionality.

Advantages :

1. Enhanced Security: The integration of multiple components, such as the ultrasonic sensor and RFID tags, provides a layered approach to security. This increases the reliability and accuracy of detecting intrusions or unauthorized access.

2. Remote Monitoring and Control: The mobile phone application enables users to remotely monitor and control the security system. This offers convenience and flexibility, allowing users to manage the system from anywhere with an internet connection.

3. Real-time Notifications: The system can send real-time notifications to the mobile phone application, keeping users informed about detected events or unauthorized access attempts. This enables prompt response and proactive actions to mitigate potential security risks.

4. User Authorization: The use of RFID tags allows for personalized access

control. Authorized individuals can easily gain access by presenting their RFID tags, while unauthorized users can be detected and flagged.

5. Integration with Existing Infrastructure: The ESP8266 WiFi module can seamlessly integrate with existing wireless networks, making it compatible with a wide range of setups and enabling easy deployment without major infrastructure changes.

Limitations:

1. Enhanced Security: The integration of multiple components, such as the ultrasonic sensor and RFID tags, provides a layered approach to security. This increases the reliability and accuracy of detecting intrusions or unauthorized access.

2. Remote Monitoring and Control: The mobile phone application enables users to remotely monitor and control the security system. This offers convenience and flexibility, allowing users to manage the system from anywhere with an internet connection.

3. Real-time Notifications: The system can send real-time notifications to the mobile phone application, keeping users informed about detected events or unauthorized access attempts. This enables prompt response and proactive actions to mitigate potential security risks.

4. User Authorization: The use of RFID tags allows for personalized access control. Authorized individuals can easily gain access by presenting their RFID tags, while unauthorized users can be detected and flagged.

5. Integration with Existing Infrastructure: The ESP8266 WiFi module can seamlessly integrate with existing wireless networks, making it compatible with a wide range of setups and enabling easy deployment without major infrastructure changes.

6. OUTCOME

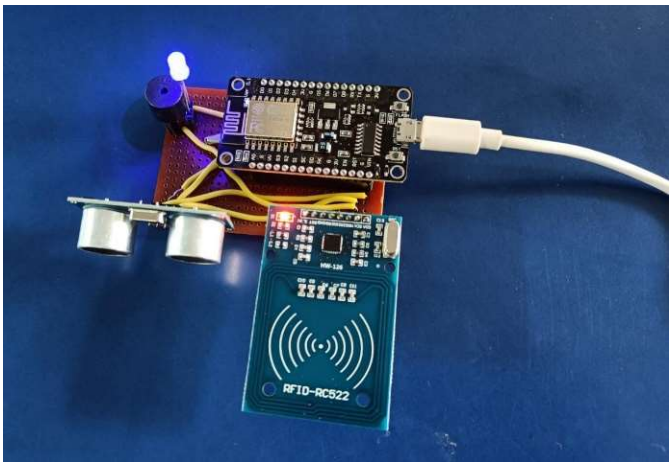

Figure 1: Circuit.

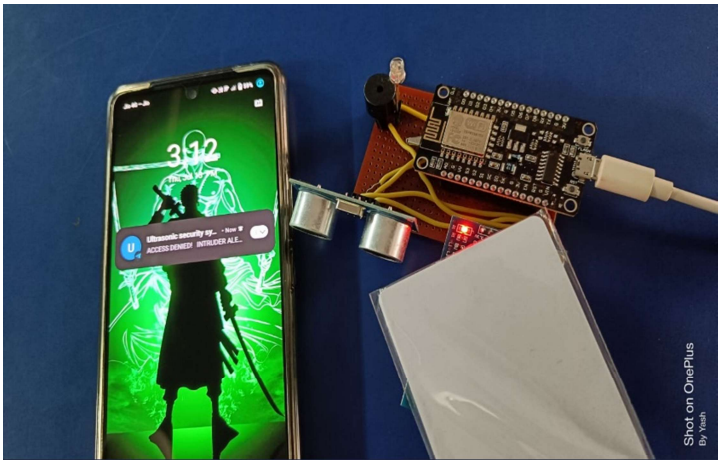

Figure 2: Access Denied due to wrong RFID tag.

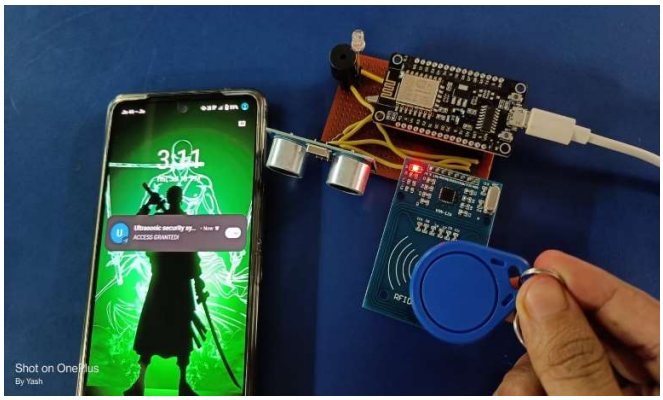

Figure 3: Access Granted for correct RFID tag.

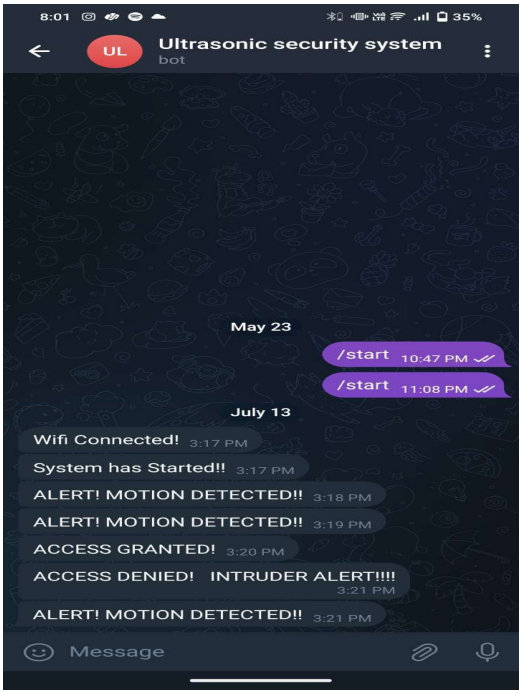

Figure 4: Telegram Bot to Receive Notifications on the Mobile Phone

7. CONCLUSIONS AND SCOPE OF THE WORK

Conclusion:

The project "Communication setup for security system using an ultrasonic sensor, ESP8266 WiFi module, and RFID tag using a mobile phone" has been successfully implemented and tested. The objective of the project was to create a reliable and efficient security system that can communicate wirelessly using ultrasonic sensors and RFID technology.

The system utilizes an ultrasonic sensor to detect the presence of any object within its range. When an object is detected, the system triggers an alert and sends the relevant information to a mobile phone using the ESP8266 WiFi module. Additionally, an RFID tag is used for authentication purposes, allowing authorized users to easily access the system.

During the implementation, several important milestones were achieved. The ultrasonic sensor was effectively integrated with the ESP8266 WiFi module, ensuring accurate detection and reliable communication. The mobile phone application was developed to receive and display the alerts sent by the system, providing real-time updates to the user. The RFID technology was successfully incorporated into the system, adding an extra layer of security and user identification.

The project's objectives were met, and the system demonstrated its effectiveness in enhancing security measures. By leveraging wireless communication and advanced technologies like ultrasonic sensors, WiFi modules, and RFID tags, the system provides a robust solution for security applications.

Future Scope:

Although the project has been successfully implemented, there are several potential areas for future improvement and expansion. Some of the future scope considerations for the project include:

1. Integration with Cloud Services: The system can be further enhanced by integrating it with cloud services. This would allow users to remotely monitor and control the security system from anywhere using their mobile devices or computers.

2. Mobile Application Enhancements: The mobile application can be enhanced to provide additional features and functionalities. This may include features such as live video streaming, event logs, and the ability to remotely arm or disarm the security system.

3. Multi-sensor Integration: While the project focused on using an ultrasonic sensor for detection, incorporating multiple sensors like infrared sensors, motion detectors, or cameras can provide a more comprehensive security solution.

4. Machine Learning and Artificial Intelligence: Implementing machine learning algorithms or artificial intelligence techniques can enable the system to learn and adapt to different scenarios, improving its accuracy in detecting and identifying potential security threats.

5. Home Automation Integration: Integrating the security system with home automation features can provide users with a centralized control hub for managing security, lighting, and other smart home devices.

6. Scalability and Expandability: The system can be designed to accommodate a larger number of sensors and devices, allowing for scalability and expandability in larger security applications.

By considering these future scope possibilities, the project can be further developed into a sophisticated and versatile security system that meets the evolving needs of users and addresses emerging challenges in the field of security technology.

REFERENCES:

https://arduino-esp8266.readthedocs.io/en/latest/esp8266wifi/readme.html

https://www.electronicwings.com/sensors-modules/esp8266-wifi-module

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://en.m.wikipedia.org/wiki/ESP8266&ved=2ahUKEwjF8KjT4I2AAxWeZmwGHckpAKAQFnoECF0QAQ&usg=AOvVaw3L74AIUBEg8vgz0YufyP4y

https://randomnerdtutorials.com/esp8266-pinout-reference-gpios/

APPENDIX

IDE CODE:

```
ultra sonic security system final code#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>
#include <SPI.h>
#include <MFRC522.h>
constexpr uint8_t RST_PIN = D3;     // Configurable, see typical pin layout above
constexpr uint8_t SS_PIN = D4;     // Configurable, see typical pin layout above
MFRC522 rfid(SS_PIN, RST_PIN); // Instance of the class
MFRC522::MIFARE_Key key;
String tag;
const char* ssid = "why5";// Enter your WIFI SSID
const char* password = "Shreyas@2002"; // Enter your WIFI Password


#define BOTtoken "6066222918:AAGNwIUOsB6UpWI80jdgjRgiroTC2OibaxA"
// Enter the bottoken you got from botfather
#define CHAT_ID "1305548944" // Enter your chatID you got from chatid bot


X509List cert(TELEGRAM_CERTIFICATE_ROOT);
WiFiClientSecure client;
UniversalTelegramBot bot(BOTtoken, client);

int const trigPin = 4;
int const echoPin = 5;
int const buzzPin = 15;


void setup() {
  Serial.begin(9600);
  SPI.begin(); // Init SPI bus
  rfid.PCD_Init(); // Init MFRC522
  pinMode(D8, OUTPUT);
  Serial.begin(115200);
  configTime(0, 0, "pool.ntp.org");
  client.setTrustAnchors(&cert);
```

```
  WiFi.mode(WIFI_STA);
  WiFi.begin(ssid, password);

  int a = 0;
  while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(500);
    a++;
  }

pinMode(trigPin, OUTPUT);
pinMode(echoPin, INPUT);
pinMode(buzzPin, OUTPUT);


  Serial.println("");
  Serial.println("WiFi connected");
  Serial.print("IP address: ");
  Serial.println(WiFi.localIP());
  bot.sendMessage(CHAT_ID, "Wifi Connected!", "");
  bot.sendMessage(CHAT_ID, "System has Started!!", "");
}
void loop() {
  int duration, distance;
digitalWrite(trigPin, HIGH);
delay(1);
digitalWrite(trigPin, LOW);
duration = pulseIn(echoPin, HIGH);
distance = (duration/2) / 29.1;
if (distance <= 10 && distance >= 0) {
digitalWrite(buzzPin, HIGH);

bot.sendMessage(CHAT_ID, "ALERT! MOTION DETECTED!!", "");

} else {
digitalWrite(buzzPin, LOW);

}
```

```
 if ( ! rfid.PICC_IsNewCardPresent())
   return;
 if (rfid.PICC_ReadCardSerial()) {
   for (byte i = 0; i < 4; i++) {
     tag += rfid.uid.uidByte[i];
   }
   Serial.println(tag);
   if (tag == "8284210207" ) {
     Serial.println("Access Granted!");

     digitalWrite(D8, HIGH);
     delay(100);
     digitalWrite(D8, LOW);
     delay(100);
     digitalWrite(D8, HIGH);
     delay(100);
     digitalWrite(D8, LOW);
     delay(100);
     digitalWrite(D8, HIGH);
     delay(100);
     digitalWrite(D8, LOW);
     delay(100);
     bot.sendMessage(CHAT_ID, "ACCESS GRANTED!", "");
     delay(30000);



 }
   else {
     Serial.println("Access Denied!");
     digitalWrite(D8, HIGH);
     delay(2000);
     digitalWrite(D8, LOW);
     bot.sendMessage(CHAT_ID, "ACCESS DENIED!   INTRUDER ALERT!!!!",
"");
   }
 }
   tag = "";
   rfid.PICC_HaltA();
   rfid.PCD_StopCrypto1(); }
```