|  |  |  |
| --- | --- | --- |
| **KONERU LAKSHMAIAH EDUCATION FOUNDATION**  **AZIZ NAGAR, HYDERABAD**  **DEPARTMENT OF ECE**  **Project Proposal** | | |
| **1.0** | **Details of Candidates:** | (i) 2310040030-AB Nitin  (ii)2310040031-G. Anurag  (iii) 2310040056-G. Pranay  (iv) 2310040072- G. Akshaya | |
| **Course of Study:** | B. TECH/ECE | |
| **Year:** | II | |
| **Semester:** | II | |
| **2.0** | **Course Details:** | |  |  | | --- | --- | |  | 23SDEC01A/R/E |   Embedded System Automation | |
| **3.0** | **Name of Supervisor:** | Mrs. Kosaraju Madhavi | |
| **4.0** | **Proposed Title:** | Bluetooth Password-Protected Door Lock using ESP32 & Arduino | |

**Introduction**

In today's world, security is a critical aspect of modern living, with increasing concerns about unauthorized access to homes, offices, and other facilities. Traditional mechanical locks, while effective, have limitations such as vulnerability to key loss, theft, and unauthorized duplication. With the rise of smart technologies, there is a growing demand for advanced, more secure, and convenient alternatives to mechanical locks. One of the most promising innovations in the field of access control is the Bluetooth-based password-protected door lock system. This system combines the convenience of wireless communication with enhanced security features, providing an efficient solution for locking and unlocking doors remotely. This project focuses on developing a Bluetooth password-protected door lock system using the ESP32 microcontroller and Arduino platform. The ESP32 is a powerful microcontroller with built-in Wi-Fi and Bluetooth capabilities, making it an ideal choice for creating wireless systems. Arduino, on the other hand, is an open-source platform widely used in embedded systems, allowing for easy integration with various sensors and components. By leveraging these technologies, the project aims to create a reliable and secure system that allows users to control access to doors through their smartphones. The system works by using Bluetooth to communicate between the mobile device and the ESP32, enabling users to remotely lock or unlock the door from a distance. The addition of a password-protected feature adds another layer of security, ensuring that only authorized individuals can gain access. This password can be set and verified through a mobile application, which interfaces with the ESP32 to trigger the door lock mechanism. By eliminating the need for physical keys, the system offers greater convenience and enhanced security compared to traditional locking mechanisms. The proposed Bluetooth-based password-protected door lock system not only addresses the shortcomings of conventional locks but also opens the door to new possibilities in smart home automation. It provides a cost-effective and efficient solution that can be easily adapted to a variety of applications, from residential buildings to offices and commercial establishments. The combination of wireless technology and password protection ensures that the system remains both secure and user-friendly, offering a significant step forward in the evolution of access control systems.

**General Introduction**

In an era where technology is advancing rapidly, traditional security methods are gradually being replaced by smarter, more efficient solutions. One such innovation is the use of Bluetooth-based access control systems, which offer enhanced security and convenience for managing physical entry points. Traditional locks, while reliable, often have limitations such as key duplication, the risk of losing keys, and the need for physical interaction. As the world becomes increasingly interconnected, there is a growing demand for smarter solutions that integrate seamlessly with everyday technology. Bluetooth technology, widely used in mobile devices, offers a reliable and secure method for wireless communication. It allows devices to communicate with each other within short-range distances, making it ideal for applications that require both security and convenience. Combining this technology with microcontrollers like the ESP32, which has built-in Bluetooth functionality, offers a unique opportunity to design intelligent systems for controlling access to various premises. One prominent application of this technology is the development of Bluetooth password-protected door locks. Such systems enable users to lock or unlock doors remotely using their smartphones or other Bluetooth-enabled devices, enhancing the ease of use while maintaining high levels of security. The integration of password protection adds an extra layer of safety, ensuring that only authorized users can gain access to a restricted area.With the rise of the Internet of Things (IoT) and home automation, Bluetooth-controlled systems are becoming increasingly popular.

**Problem Statement**

The traditional method of securing doors with mechanical locks and keys presents several challenges, including the risk of key duplication, loss, or theft, as well as the inconvenience of carrying physical keys. Additionally, conventional locks require manual operation, which may not always be feasible or secure, especially in situations where quick access is necessary. As technology evolves, there is a growing need for more secure, efficient, and user-friendly alternatives to traditional locking mechanisms. In this context, Bluetooth-based access control systems have emerged as a promising solution, offering the ability to remotely control locks through wireless communication. However, many existing Bluetooth-enabled door locks are either too expensive, lack adequate security features, or are not easily customizable for different use cases. The problem, therefore, is to design a Bluetooth password-protected door lock system using the ESP32 microcontroller, which provides a reliable, secure, and cost-effective solution for controlling access to doors. The system should integrate Bluetooth communication for remote operation and incorporate password protection to ensure only authorized users can access the locked area. The challenge lies in ensuring that the system is both user-friendly and robust enough to handle various security threats while maintaining ease of use and affordability. This project aims to address these concerns by developing a Bluetooth-based door lock system that is secure, simple to operate, and scalable, with the potential for integration into home automation systems and other IoT-based applications.

**Objectives of the study**

The primary objectives of this study are:

**Design and Implementation:** To develop a Bluetooth password-protected door lock system using the ESP32 microcontroller that can control access to a door remotely via a Bluetooth-enabled device (smartphone). Security Enhancement: To enhance security by integrating a password mechanism, ensuring that only authorized users can access the door, reducing the risks associated with traditional locks. User-Friendly Interface: To create a user-friendly system that allows easy operation, installation, and maintenance, enabling users to remotely unlock the door using an application on their smartphones. Cost Efficiency: To design a cost-effective solution that leverages affordable hardware and software, making the system accessible for a wide range of users without compromising on security. Scalability and Integration: To ensure that the system can be easily integrated into larger home automation or security networks, providing a scalable solution for multiple access points.

**Scope of the Project**

This project focuses on the development of a Bluetooth-based, password-protected door lock system using the ESP32 microcontroller. The scope includes:

Bluetooth Integration: Utilizing the Bluetooth capabilities of the ESP32 to facilitate wireless communication between the door lock and a mobile device.

Password Protection: Implementing a password mechanism for enhanced security to ensure that only authorized users can operate the lock.

Control and Monitoring: Allowing remote control of the lock from a smartphone app, including the ability to lock and unlock the door and manage access.

User Interface: Designing a simple mobile application interface for users to enter the password and control the lock.

Security Features: Addressing potential vulnerabilities in Bluetooth communication and ensuring the system remains resistant to unauthorized access attempts.

This project will not include advanced features such as biometric authentication or Internet of Things (IoT) cloud integration but will focus on providing a robust, cost-effective, and secure solution for Bluetooth-based door access control.

**Literature Review**

**Introduction**

The rapid evolution of Internet of Things (IoT) technologies has brought about innovative solutions for everyday problems, including security. One area where IoT has shown significant promise is in the development of smart locks. These digital locking systems integrate wireless communication, such as Bluetooth, to replace traditional mechanical locks, offering greater security, convenience, and customization. However, while there are many solutions in the market, security concerns, ease of use, and affordability remain areas that require further exploration.

**Existing Technologies and Methods**

Several Bluetooth-based locking systems have been developed in recent years, with many focusing on security features like encryption, password protection, and remote access via mobile apps. These systems typically rely on Bluetooth Low Energy (BLE) for communication, offering benefits such as low power consumption and quick response times. However, issues like weak encryption, vulnerability to hacking, and reliance on centralized cloud services are significant challenges that need addressing. Existing solutions such as smart locks from brands like August, Schlage, and Yale offer convenience but come at a premium cost. These locks often require additional subscription fees for cloud services, which may not be appealing to all users.

**Prior Research and Theoretical Background**

Studies on smart locks and access control systems have examined various communication protocols, including Bluetooth, Wi-Fi, and Zigbee. Research has highlighted the importance of incorporating strong encryption methods to prevent unauthorized access and ensure that data exchanged between the lock and the mobile device is secure. Additionally, the use of low-power devices like the ESP32 in such systems has been emphasized due to their ability to operate efficiently in battery-powered scenarios. One key area of focus in research has been developing systems with two-factor authentication, where users must provide a password or PIN in addition to Bluetooth communication, to enhance security further.

**Research Gaps and Project Relevance**

While existing technologies address certain aspects of Bluetooth-based door lock systems, there are gaps in terms of affordability, user experience, and security. Many commercial systems are expensive, and their security mechanisms, although robust, may not be foolproof. This project aims to fill these gaps by developing an affordable and secure system using widely available hardware like the ESP32 and incorporating password protection for added security.

**Theoretical Implications and Practical Applications**

The theoretical implications of this project include the application of secure communication protocols, efficient power management techniques, and secure password authentication. In practical terms, this research can be applied to home security, office access control systems, and even advanced IoT-based automation setups, where door access control is integrated with other smart systems.

**Summary of Literature and Path Forward**

In summary, while the development of Bluetooth-based smart locks has been well-researched, there remain opportunities to improve affordability, security, and user experience. This project seeks to build on existing knowledge by focusing on a cost-effective, password-protected solution using the ESP32, with an emphasis on Bluetooth communication and practical security measures. The path forward involves the design, development, and testing of the proposed system to address the identified gaps and provide a viable solution for users seeking enhanced door security.

**Abstract:**

This project focuses on the development of a Bluetooth password-protected door lock system using the ESP32 microcontroller. The system is designed to offer an affordable and secure alternative to traditional mechanical locks, leveraging Bluetooth Low Energy (BLE) for wireless communication. The main objective is to provide users with a convenient, remote-controlled locking mechanism, which can be accessed via a smartphone app. The system is protected by a password mechanism, ensuring that only authorized individuals can gain access to the secured area. The ESP32 microcontroller, known for its low power consumption and powerful processing capabilities, serves as the core of the system, facilitating communication with the mobile app and controlling the door lock. The app interface allows users to enter a password to unlock the door, enhancing security by preventing unauthorized access. Additionally, the project aims to ensure that the system remains scalable, enabling future integration with other home automation systems. This project addresses security concerns associated with conventional door locks and offers a simple yet effective solution for modern access control. The research emphasizes the importance of password protection, encryption, and ease of use, contributing to the growing field of IoT-based smart security systems

**Methodology**

The methodology for this project will involve a series of well-defined steps to design, develop, and test the Bluetooth password-protected door lock system. The process can be divided into several key phases:

**System Design**

Hardware Selection and Setup:

ESP32 Microcontroller: The ESP32 microcontroller will be selected as the main controller for the system due to its Bluetooth capabilities, processing power, and low power consumption. The ESP32 will be responsible for Bluetooth communication, password verification, and controlling the relay that operates the door lock.

Bluetooth Module: The ESP32 has an in-built Bluetooth module that will be utilized for communication with the smartphone app.

Door Lock Mechanism: A solenoid or servo motor will be used to physically lock and unlock the door when commanded by the microcontroller.

Power Supply: The system will require a stable power supply to ensure continuous operation of the microcontroller and the locking mechanism.

Software Development: Firmware Development for ESP32: The firmware for the ESP32 will be developed using the Arduino IDE. The code will handle Bluetooth communication, password management, relay control, and security protocols.

Mobile App Development: A simple mobile app (either custom-developed or using pre-existing frameworks like Blynk) will be used to send commands to the ESP32. The app will allow users to input a password and control the lock remotely.

Security and Communication Protocol

Password Protection:

The system will require the user to input a password to unlock the door. This password will be stored securely on the ESP32 microcontroller and compared with the entered password.

If the entered password matches the stored password, the system will send a signal to the door lock mechanism to unlock the door.

Bluetooth Communication:

The communication between the mobile device and the ESP32 will be established using Bluetooth Low Energy (BLE). The app will connect to the ESP32, send the password, and receive the corresponding feedback (whether the door is unlocked or locked).

Encryption and Security:

Basic encryption techniques will be applied to the password to ensure secure transmission over Bluetooth. Additionally, the communication between the app and the ESP32 will be protected against unauthorized access.

System Integration

Once the individual components (hardware and software) are developed, the system will be integrated. The ESP32 will be programmed to handle the password authentication, Bluetooth communication, and control the locking mechanism. The mobile app will be integrated to interact with the ESP32 and provide a user-friendly interface for password input and door control.

Testing and Validation

Functionality Testing:

The system will undergo thorough testing to ensure that the Bluetooth communication is stable, the password system functions correctly, and the door lock operates as expected.

Different password scenarios will be tested to verify the accuracy of the password matching process and ensure that unauthorized access attempts are prevented.

Security Testing:

Security testing will be conducted to assess the robustness of the password protection and encryption used in the system.

Attempts to bypass the password mechanism and access the system through unauthorized means will be performed to evaluate the system’s resistance to hacking.

Performance Testing:

The performance of the system, including response time, battery life, and stability, will be assessed under different operational conditions.

**Financial Arrangements**

The budget is given below:

|  |  |  |  |
| --- | --- | --- | --- |
| S.NO | Component | Description | Cost |
| 1 | ESP32 Board (with built-in Bluetooth) | A microcontroller with built-in Wi-Fi and Bluetooth functionality, ideal for IoT projects. | 500 |
| 2 | Solenoid Lock (12V) | An electronically controlled lock that requires a 12V power supply to lock or unlock the door. | 600 |
| 3 | TIP120 Darlington Transistor | A power transistor used to control the solenoid lock by switching it on/off. | 20 |
| 4 | Diode(for Back EMF Protection) | A diode is used to protect the circuit from voltage spikes caused by the solenoid lock. | 10 |
| 5 | Resistors (1kΩ to 3kΩ) | Resistors are used to prevent high voltage from damaging the ESP32 and for voltage regulation in the circuit. | 10 |
| 6 | External 12V Power Supply | An external power supply required to power the solenoid lock. | 300 |
| 7 | Bread Board | A prototyping board for building and testing circuits without soldering. | 100 |
| 8 | Jumper wires | Wires used to make connections between components on the breadboard. | 100 |
| 9 | Resistors (for Voltage Protection) | Additional resistors required for wiring and voltage protection in the circuit. | 10 |
|  |  | Grand Total | 1650 |

**References**

**Jiang, H., & Zhang, L.** (2020). "Design and Implementation of a Smart Door Lock System Based on IoT." *International Journal of Computer Science and Network Security*, 20(4), 35-42.

This paper presents an IoT-based smart door lock system, exploring various security

protocols and communication methods like Bluetooth and Wi-Fi. It provides insights into

secure communication methods for IoT-based access control systems.

**CANDIDATES**

Name: AB Nitin, Reg. No. 2310040030

Signature: ……………………… Date: …………

Name: G. Anurag, Reg. No.2310040031

Signature: ……………………… Date: …………

Name: G. Pranay, Reg. No. 2310040056

Signature: ……………………… Date: …………

Name: G. Akshaya, Reg. No. 2310040072

Signature: ……………………… Date: …………

**SUPERVISOR**

1. Comments by Supervisor:

………………………………………………………………………………………………………

……………………………………………..…………………………..……………………………

………………………………………………………………………………………………………

……………............................................

Date: ……............ Name: ……....……….…………..

Signature: .…………………........