

Smart Locking System

Hüseyin Emir KIR

Supervisor Prof.Dr. Sema KAYHAN



Department of Electrical and Electronics Engineering, University of Gaziantep, Turkey.

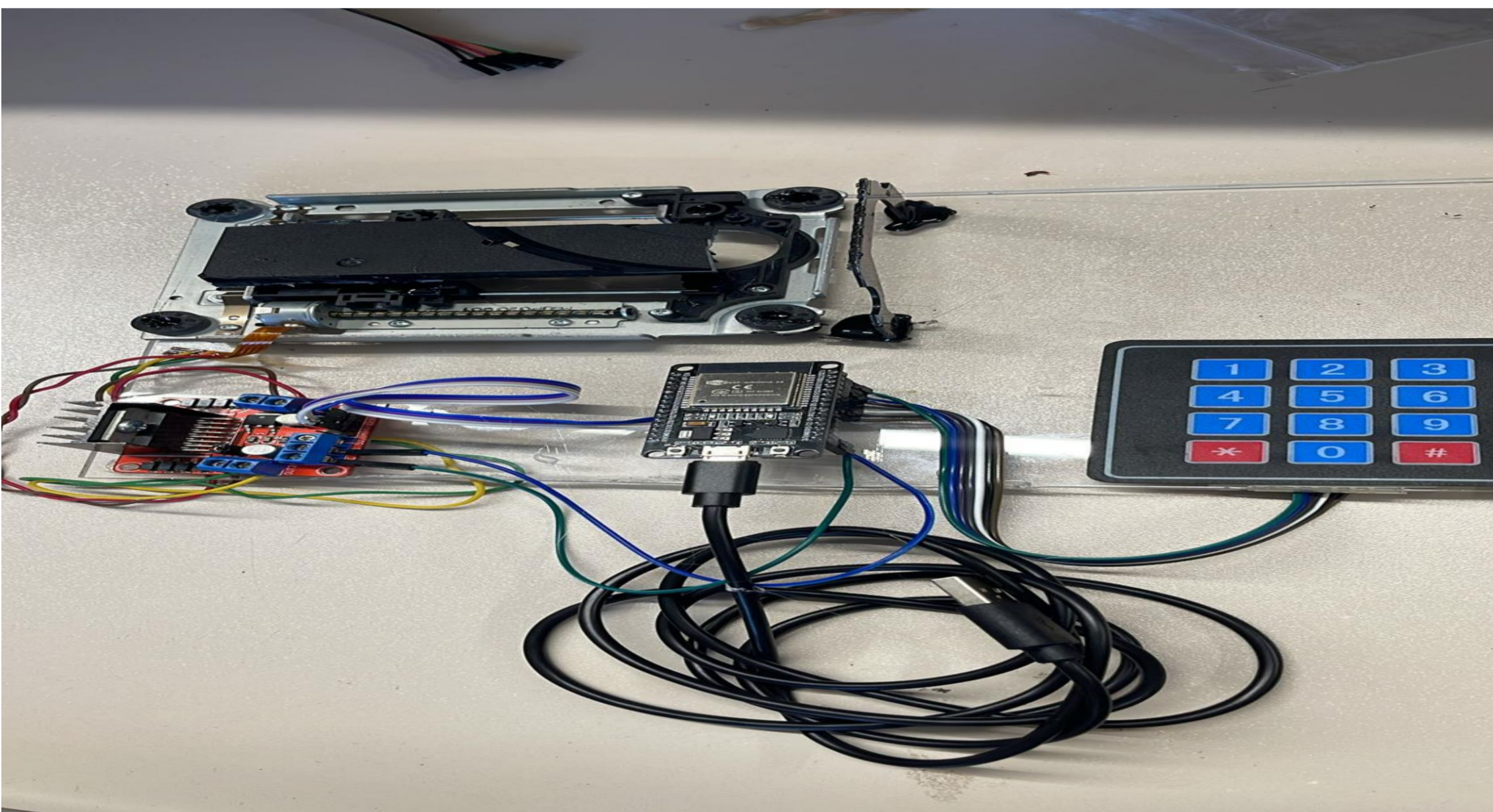
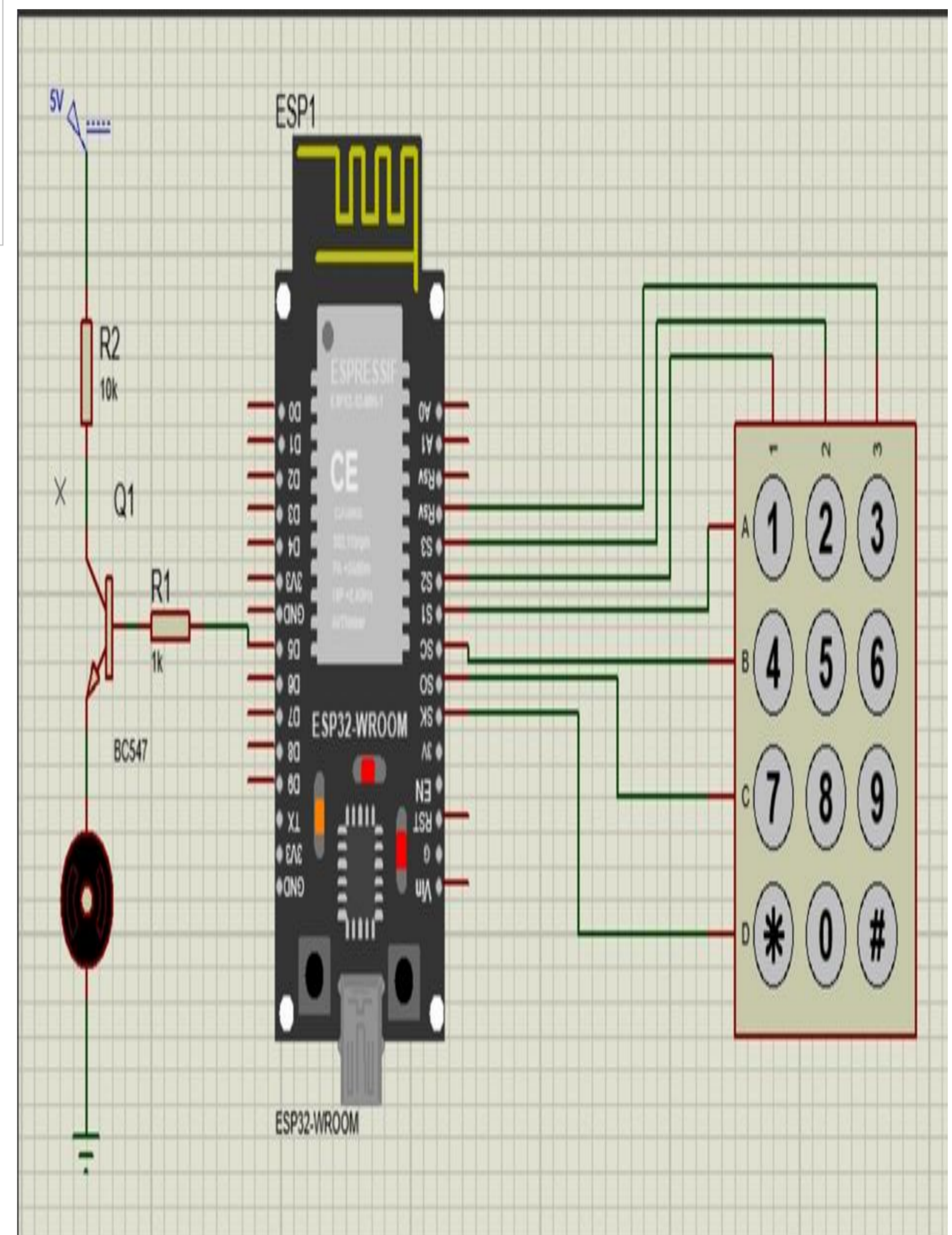
Abstract

This project addresses the design and implementation of a password-controlled door lock system using a 4x3 keypad, Wi-Fi module and BLE Bluetooth module. The system opens the door when the correct password is entered, and remains closed when the wrong password is entered. The 4x3 keypad allows users to enter passwords, while the Wi-Fi module and BLE Bluetooth module are used for remote access and control. In this way, users can manage the door lock securely both locally and remotely. The aim of the project is to increase the effectiveness of access control systems by providing a reliable and user-friendly security solution. The system can be easily implemented using low-cost components and adapted to various security scenarios.

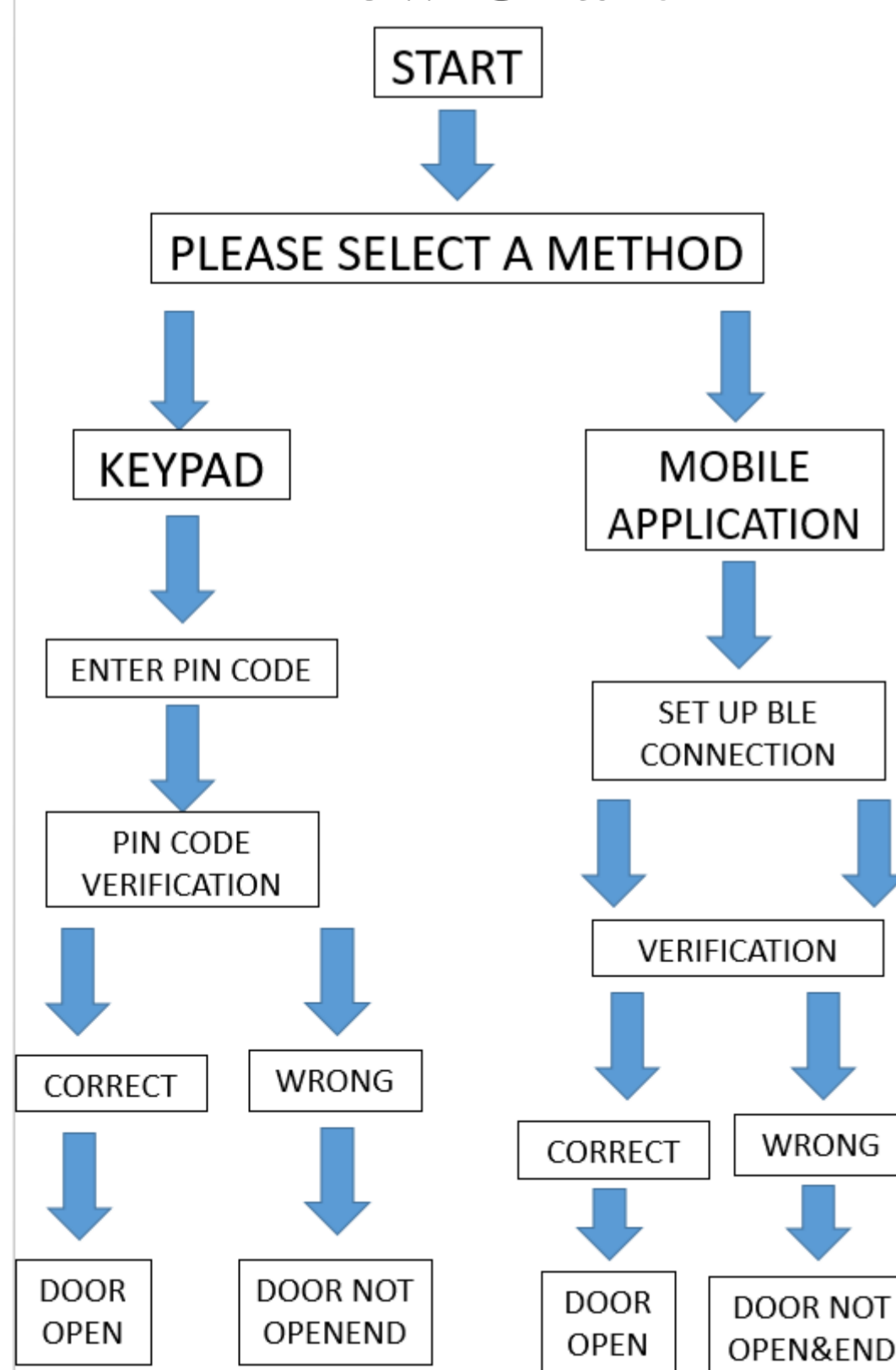
Main Components

ESP32-WROOM, Wifi Module, Ble Module , DC Motor ,5V 1A Power Supply

Electrical Design



Flow Chart



Conclusion

In conclusion, The smart lock project combines the ESP32-WROOM-32 microcontroller, 3x4 keypad, BLE Bluetooth module, Wi-Fi module, and a DC motor to create a secure and versatile access control system. The lock opens with the correct password (1524) and can also be controlled via Wi-Fi and Bluetooth. The project met key design criteria, including reliable sensor sensitivity, fast response times, user-friendly calibration, energy efficiency, and system stability. Its modular design allows for future upgrades, and it was completed within budget. This project successfully integrates modern communication protocols with traditional locking mechanisms, providing a practical and secure solution..

References:

- Lee, S., & Lee, J. (2018). Proximity-based unlocking mechanisms using Bluetooth Low Energy. *Wireless Communication and Networks Journal*, 22(4), 289-302.
- Kim, S., Lee, J., & Choi, Y. (2020). Addressing security challenges in smart lock systems. *International Journal of Cyber Security*, 9(1), 45-58