EN2160 - Electronic Design Realization

Avishka Herath - 200212F

herathhmeac.20@uom.lk

University of Moratuwa — July 30, 2023

Department of Electronic and Telecommunication Engineering

Semester 4 (Intake 2020)

Final Project Report

RFID Based Access Control and Smart Attendance System

This document is submitted as a partial fulfillment of the module EN2160 - Electronic Design Realization.

Contents

Abstract

This project report presents the development and evaluation of an innovative RFID-based Access Control and Attendance System (RAAS) with Wi-Fi connectivity, designed to enhance security and streamline attendance tracking in various organizational settings. Combining advanced RFID technology and smart features, the system efficiently manage access permissions and automate attendance recording, mitigating traditional manual processes' shortcomings.

The report begins with an overview of existing access control and attendance management methodologies, highlighting their limitations and the need for a more sophisticated and automated solution. The theoretical foundation encompasses key concepts of RFID technology, access control algorithms, and database management systems, laying the groundwork for the proposed system's architecture.

To address the requirements, the system incorporates advanced RFID technology to provide secure and seamless access control. Employees are granted access via RFID tags, while real-time attendance data is automatically transmitted over Wi-Fi for instant updates. Administrators gain remote access to monitor access events and attendance records, facilitated by cloud integration, ensuring data availability, backup, and analysis.

These systems are utilized in various real-world applications, including corporate offices to restrict access to sensitive areas, educational institutions for automated attendance tracking, hospitals to secure critical areas and patient information, research facilities for laboratory security, public transport for quick entry and exit, warehouses to manage inventory, event management for secure entry and cashless transactions, libraries for book tracking, government facilities for restricted areas, and residential/commercial buildings for secure access to common areas and individual units. RFID technology's versatility continues to drive its adoption across industries, offering enhanced security, efficiency, and convenience.

In conclusion, this project report highlights the successful development and implementation of an RFID-based Access Control and Smart Attendance System. The system's seamless integration with smart features and Wi-Fi connectivity, the system presents a forward-thinking approach to address modern organizational needs. The successful implementation of this system will yield enhanced security, streamlined attendance management, and improved operational efficiency across diverse sectors. Future work will focus on scalability for larger deployments and continued exploration of cutting-edge technologies to augment the system's functionality and adaptability.

Part I
Problem identification, ideation and concept development

1 Problem statement

1.1 Overview of the issue

The current access control and attendance tracking methods in organization rely on traditional RFID technology and manual recording, which can still lead to inefficiencies and limited functionalities. To address these limitations and further enhance security and convenience, there is a need to develop an RFID-Based Smart Access Control and Attendance System with Wi-Fi connectivity.

1.2 Requirements for problem solving

The project aims to develop an advanced RFID-based solution with Wi-Fi connectivity to meet the following requirements:

a) Secure and seamless access control: The system should employ advanced RFID technology for secure access, eliminating the need for physical contact while offering real-time identification.

b) Smart attendance tracking: Utilizing RFID technology, the system should automatically track attendance and transmit data over Wi-Fi for instant updates.

c) Real-time monitoring and remote access: The smart system should allow administrators to monitor access events and attendance remotely through Wi-Fi connectivity.

d) Cloud integration: Attendance data should be securely stored in the cloud, ensuring easy access, backup, and analysis.

e) Mobile application compatibility: Employees should be able to use a mobile application to view attendance records and receive notifications.

2 Existing product analysis

2.1 Examination of current solutions

The current RFID-based access control systems organization offer basic security but lacks smart features and Wi-Fi connectivity. Attendance tracking is done manually or through limited integration with databases, resulting in delayed updates.

Access Control System Safe Electronic Gate Opener Home Garage Digital Set Eletric Magnetic RFID Smart Door Lock Kit - AliExpress

2.2 Features of established products

While some organizations have adopted Wi-Fi-enabled access control systems, they often lack integration with RFID technology. Additionally, attendance management and remote access capabilities might be limited. General product specifications on market available products:

- Card read distance: 0 - 10 cm
- RF type: EM card
- Working temperature: -10 - 70 $^{\circ}\mathrm{C}$
- Memory: 250 standard users

3 Proposed enhancements

3.1 Innovations to incorporate

The proposed RFID-Based Smart Access Control and Attendance System will be a significant technological advancement. It will utilize Wi-Fi connectivity to enable real-time data transmission and remote monitoring. Furthermore, the proposed specifications and features to incorporate will be:

- Increased sensitivity and security: Advanced authentication and encryption to ensure heightened sensitivity and security, protecting sensitive data and access control mechanisms in the system.
- Integration of a Database: Development of a web-page to indicate real time status of a user by using a real time database.
- Wi-Fi connectivity: Seamless connectivity of Wi-Fi 2.4 GHz, support WPA/WPA2
- Power efficiency: Optimize power consumption and to be able to change into idle mode when an RFID tag is not in the range.

3.2 Additional features for consideration

- IoT based security system: Sending real-time notifications to the user whenever he enters using the card. This feature would help manage administrators for critical access events or attendance anomalies.
- Kit based product: Integrating a Solenoid Lock and a Proximity Sensor separate parts of the product with the ability to connect as required.
- Advanced analytics and reporting: Utilizing cloud-stored data to generate insightful reports and optimize resource allocation.

By developing the RFID-Based Access Control and Smart Attendance System with Wi-Fi connectivity, the system will provide enhanced security, seamless attendance tracking, and improved operational efficiency. The inclusion of smart features will pave the way for a futuristic, technologically advanced access control and attendance management solution that aligns with modern-day requirements.

Part II
Detailed design and prototyping

4 Design idea generation

4.1 RFID sensor for user identification

Integration of an RFID sensor into the product enables convenient and secure user identification. The RFID technology allows for contactless communication with RFID tags or cards, providing a unique identification mechanism. This feature finds application in various scenarios, including access control systems and attendance tracking. An MFRC522 RFID module operating at 13.56 MHz was used as the sensor module. It is connected to the micro-controller through the SPI communication interface, and a unique user ID (UID) is read. A decimal equivalent of the UID is then generated using the micro-controller.

4.2 Real time database integration with Wi-Fi

Enable real-time database integration by incorporating Wi-Fi connectivity. This integration facilitates seamless data collection, storage, and processing in real-time. Users' interactions or inputs are instantly transmitted and stored, allowing for dynamic updates and synchronization across multiple devices. This feature enables remote monitoring and management of the product, offering enhanced user experiences and control.

Google Firebase is used for the real-time database. The generated UID from the micro-controller is sent to the web server through Wi-Fi using the ESP12F micro-controller, which has built-in Wi-Fi connectivity (uses an ESP8266 chip). The stored data, including the number of times accessed, entry/exit time, live status of the user, and the location used to access a particular door, is displayed on a web page that can be viewed by the administrator.

4.3 OLED and Buzzer to display output results

Enhance the product's output display capabilities with an OLED screen and a buzzer. The OLED displays high-quality visuals while consuming less power, effectively presenting output results, status updates, and user interface elements. The addition of a buzzer provides audio cues that complement the visual feedback, improving user interaction. These features contribute to an enriched user experience, intuitively and effectively conveying output results and feedback.
The buzzer's tone and time of operation are determined by whether access is granted or denied for a particular user, depending on whether they are registered in the system or not.

5 Functional block diagram

The proposed block diagram illustrates the core functionality of the system and identifies its essential components.

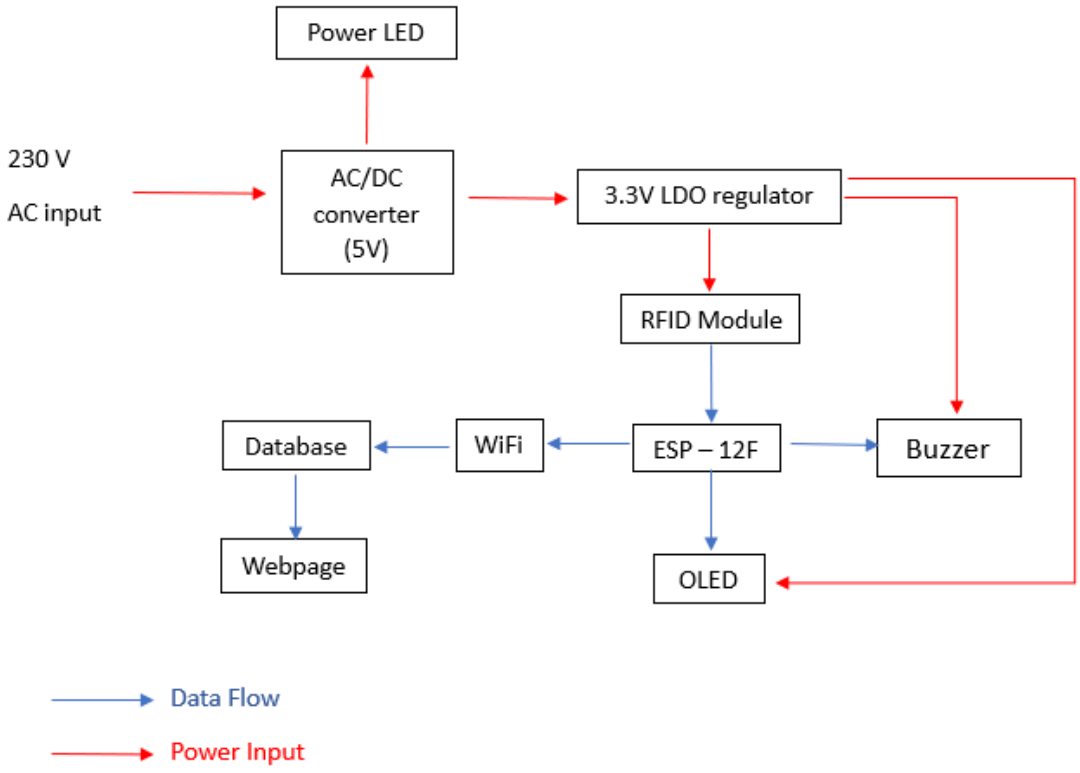


Figure 1: Functional block diagram

6 Operation and functionality of the design

The RFID-based Access Control and Smart Attendance System is designed to provide secure access control and automated attendance tracking operates as follows:

6.1 User Identification and Enrollment

Each authorized user is provided with an RFID tag or card containing a unique identifier. The RFID tag is in the form of a card. To enroll users, their information is linked to their RFID tag in the system's database.

6.2 Access Control

When a user approaches an entry point, such as a door or turnstile, the RFID reader detects the RFID tag's presence within its proximity. The RFID reader then sends the unique identifier to the system's control unit for verification. At this stage the OLED displays a "Scanning..." message.

6.3 User Verification

The system's control unit verifies the received RFID tag's identifier by cross-referencing it with the real-time database of enrolled users. If the identifier is authorized, access is granted, and a "ACCESS GRANTED" message is displayed while the buzzer emits a specific tone. In case the identifier is not recognized as authorized, access is denied to prevent unauthorized entry. In this scenario, a "ACCESS DENIED" message is displayed, and the buzzer sounds a different tone to indicate unauthorized access.

6.4 Automated Attendance Tracking

As users enter or exit the premises, their RFID tags are read, and the system automatically updates their attendance records in the database. The records consist of the number of times accessed, the time of entry or exit, the live status of the user, and the location used for access.

6.5 Real-Time Monitoring and Reporting

The web page displays the real-time status of all users, providing up-to-date information on their attendance. Additionally, the system allows users to export reports, enabling them to obtain the attendance history for specific sets of events.

7 Component selection

To fulfill the system's requirements, the following components are selected:

- **PBO-3C-5 PCB mount AC-DC converter:** This PCB mount AC-DC converter converts 50Hz 230V input voltage to a stable 5V DC output voltage. It provides a maximum output current of 600mA, which is sufficient for the circuit's operation.

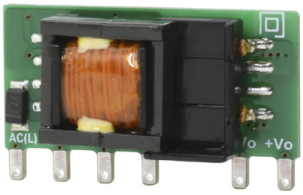


Figure 2: PBO-3C-5 PCB mount AC-DC converter

- **ESP12F Wi-Fi module:** The ESP8266 microcontroller is selected for its robust processing capabilities and integrated Wi-Fi connectivity. Its ample computing power allows efficient management of UID reading and smooth data transmission to the servers. Additionally, the ESP8266's ability to connect with nearby Wi-Fi access points ensures seamless web integration, enhancing the system's overall functionality.

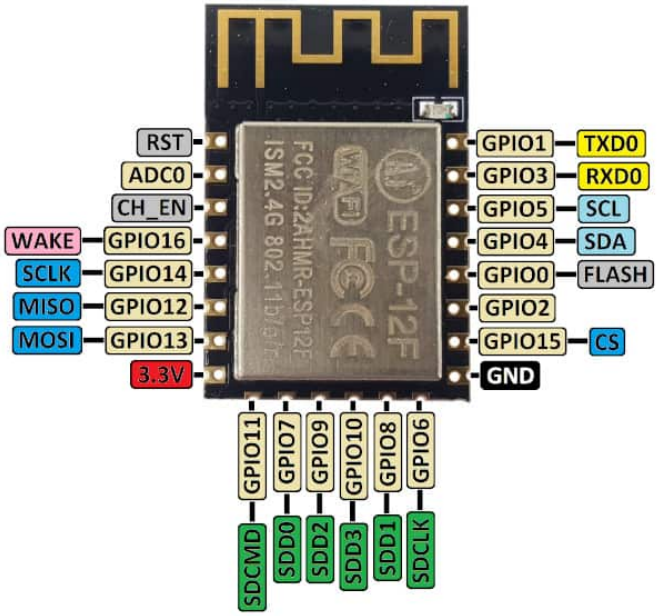


Figure 3: ESP12F Wi-Fi module

- **MFRC522 RFID module:** Operating at a frequency of 13.56 MHz with a sensitive radius of approximately 5cm, this module enables the identification of unique IDs available in NFC cards and sends the data as input to the microcontroller.

Figure 4: MFRC522 RFID module

- **SSD1306 128x64 OLED:** This OLED display is used to present the current status to the user. It was selected for its compact size and relatively higher resolution, providing clear and concise information.

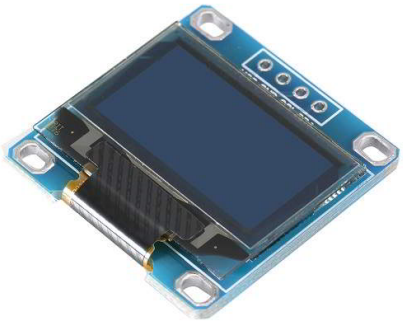


Figure 5: SSD1306 128x64 OLED

- **LM1117-3.3 Low-Dropout Linear Regulator:** The voltage regulator ensures a stable and regulated power supply to the ESP12F chip and other system components, including the RFID module and ESP12F module. With its fixed 3.3V output voltage, it perfectly matches the ESP8266's power needs, ensuring consistent and dependable operation.

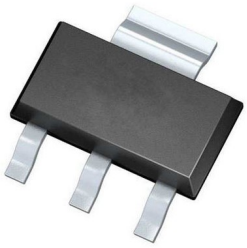


Figure 6: LM1117-3.3 Low-Dropout Linear Regulator

- **Transistor controlled Magnetic Buzzer:** A CMI-1295IC magnetic buzzer is used in conjunction with an NPN transistor (BC848B) and a Schottky flyback diode (RB501SM) to drive the buzzer and prevent voltage spikes. The buzzer cannot be directly coupled with the ESP8266 due to its GPIO current limitation of 12mA output, while the buzzer operates with a current of 30mA.

Figure 7: Magnetic Buzzer

- **Power LED:** A 3.2V 30mA blue LED is used to indicate the circuit's power status.
- **Pull up/down resistors and capacitors:** Several pull-up/down resistors are selected based on the ESP8266's datasheet to ensure proper communication and programming. Additionally, several capacitors are used to increase power stability and reduce noise in the circuit.

The careful selection of these components ensures the efficient operation and performance of the RFID-Based Access Control and Smart Attendance System.

8 Schematic design

8.1 Power supply and Regulation section

- Input voltage: 230V 50Hz
- Output voltage: 3.3V
- Maximum output current: 600mA
- Operating temp: -40 °C to +85 °C
- Emission / Immunity class: Class A / Class III

Note - R_1 must be a wire-wound resistor; do not use a chip or carbon film resistor.

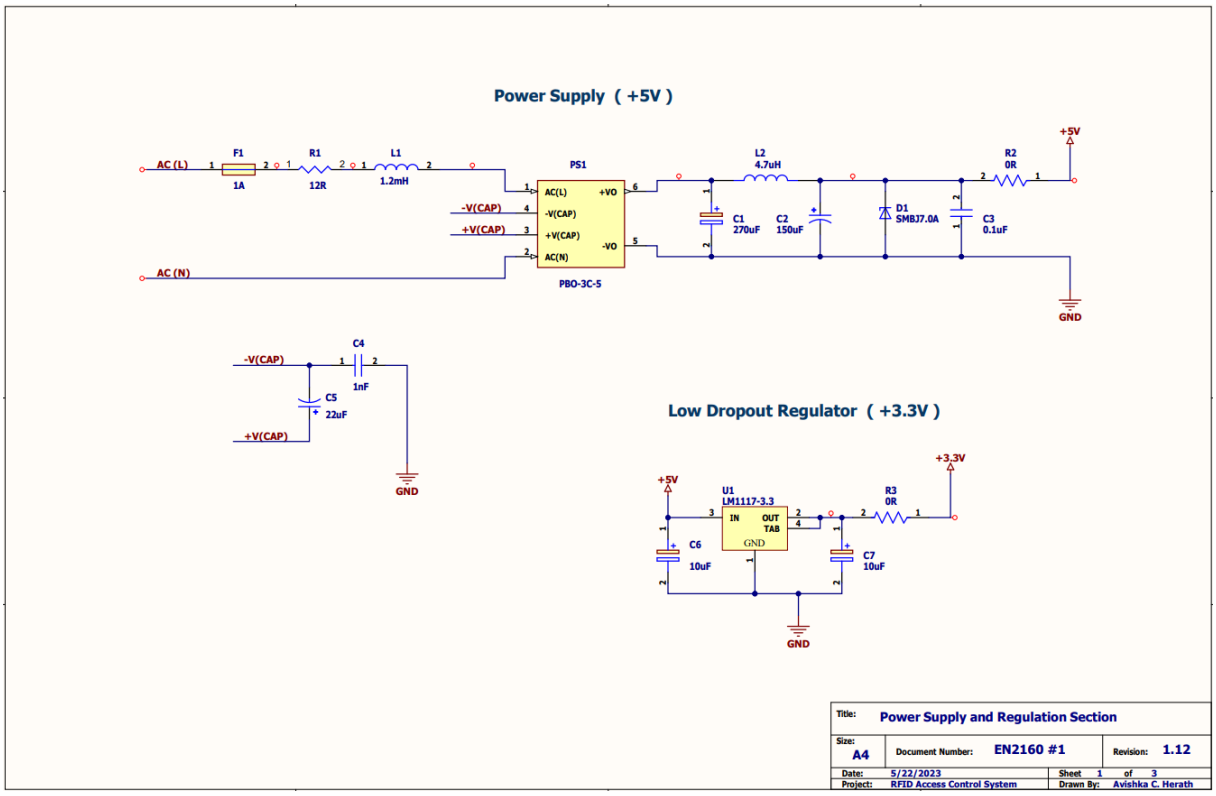


Figure 8: Power supply and Regulation section

8.2 IO and MCU section

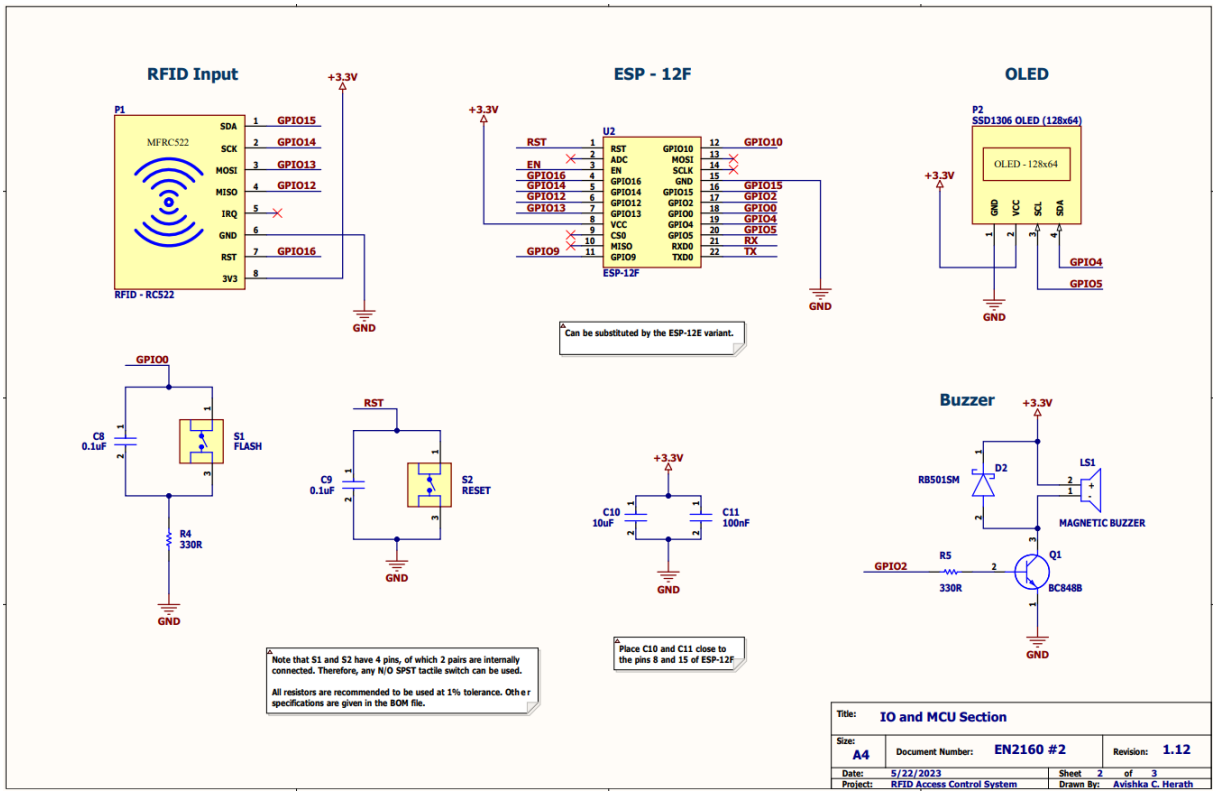


Figure 9: IO and MCU section

8.3 External connections section

Note - R_8, R_9, and R_{15} are optional.

9 PCB design

The PCB design incorporates the mentioned components while adhering to standard trace width calculations based on current requirements. Components are strategically positioned to ensure easy access and minimize potential signal interference. For instance, reset buttons are placed near the enclosure for convenient accessibility. Pull-up resistors are positioned close to the ESP12F module, facilitating efficient RX and TX processes during code uploading by reducing noise. Decoupling capacitors are placed near relevant components to mitigate voltage variations caused by noise. Additionally, ground polygon pours are added to further reduce cross-talk and maintain signal integrity.

All PCB designing was completed using Altium Designer version 23.4.

9.1 Design constraints and rules

- Board size: 70.5mm $\times$ 93.5mm
- Trace width:
  - AC net: 60mil
  - Power traces: 40mil
  - Signal traces: 20mil

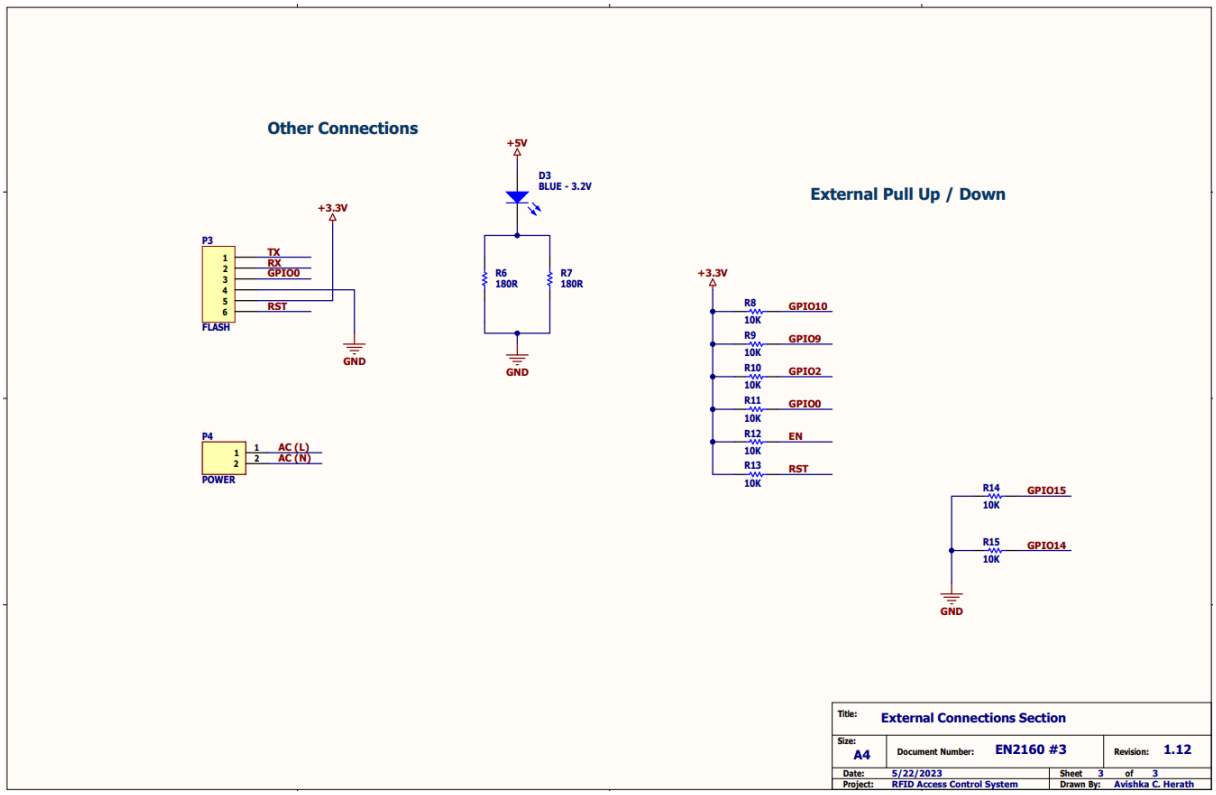


Figure 10: External connections section

- Clearance: 0.5mm (max)
- Hole size: 0.4mm (min)
- Via diameter: 0.6mm (preferred)
- Component placement: Components are strategically positioned to avoid signal interference and provide optimum shielding. The power supply unit is placed in the corner to prevent power line interference.

Note - The ESP8266s' design was routed based on the hardware design guidelines provided.

The required Rules Files can be found in the following link: https://github.com/avishkaherath/RFID-Access-Control-System/blob/main/PCB%20(Altium)/Main_v2.RUL

9.2 Top layer

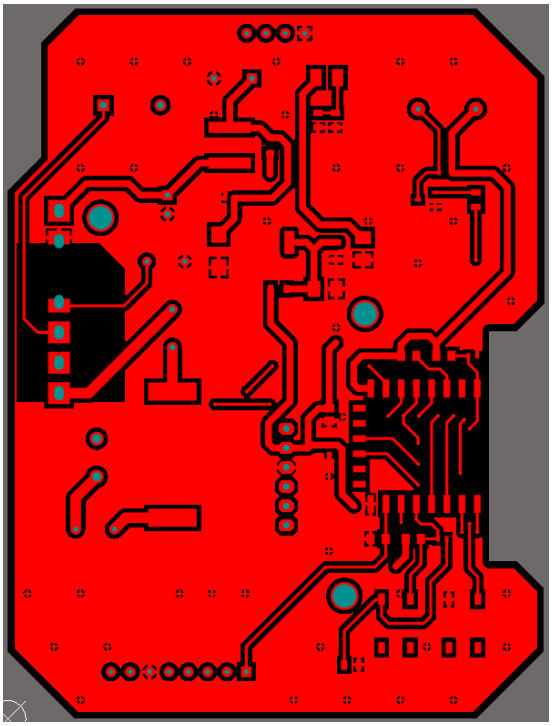


Figure 11: Top layer

9.3 Bottom layer

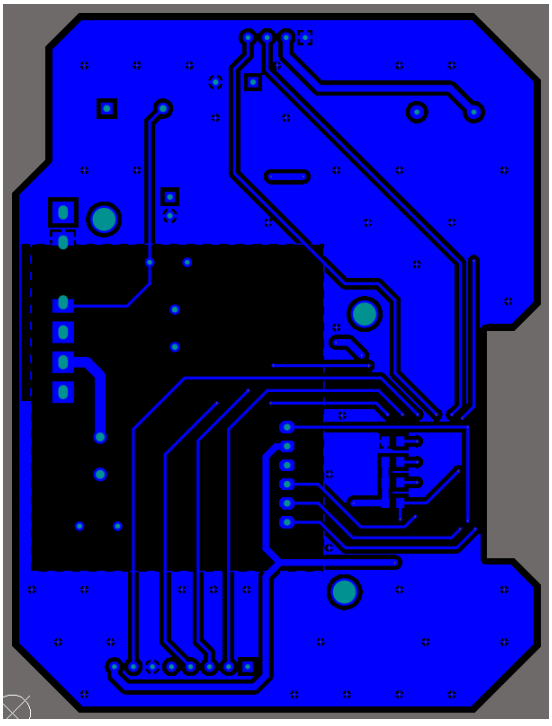


Figure 12: Bottom layer

9.4 Top overlay (silkscreen)

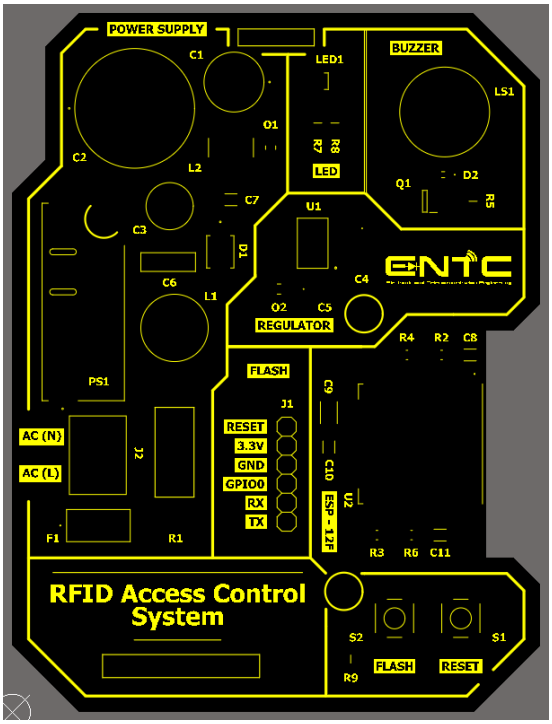


Figure 13: Top overlay

9.5 Bottom overlay

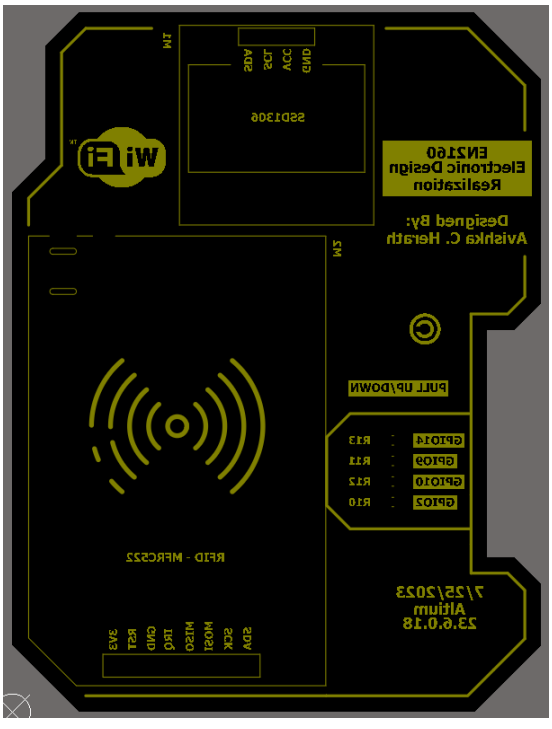


Figure 14: Bottom overlay

9.6 Top soldermask

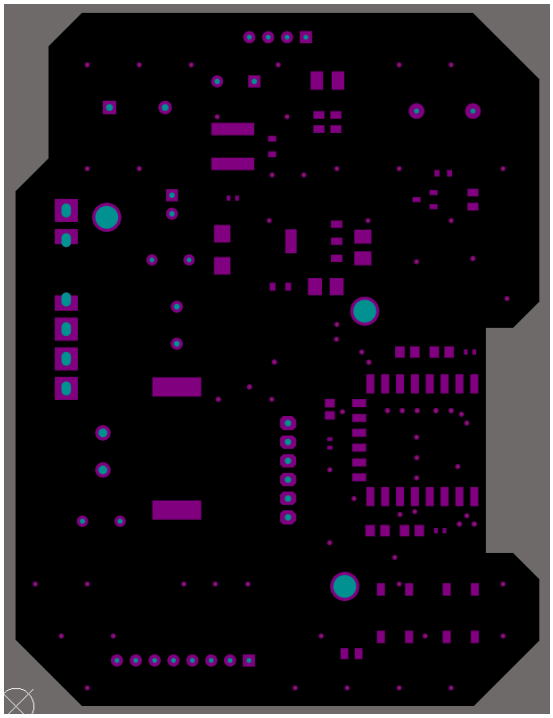


Figure 15: Top soldermask

9.7 Bottom soldermask

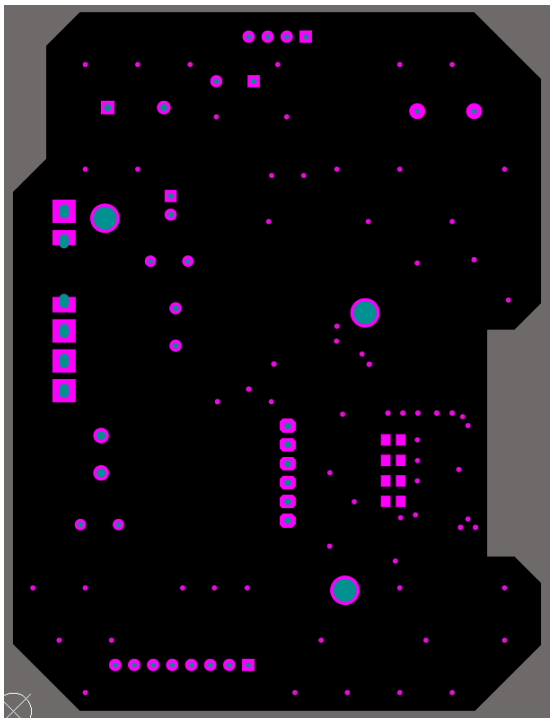


Figure 16: Bottom soldermask

9.8 Top 3D view

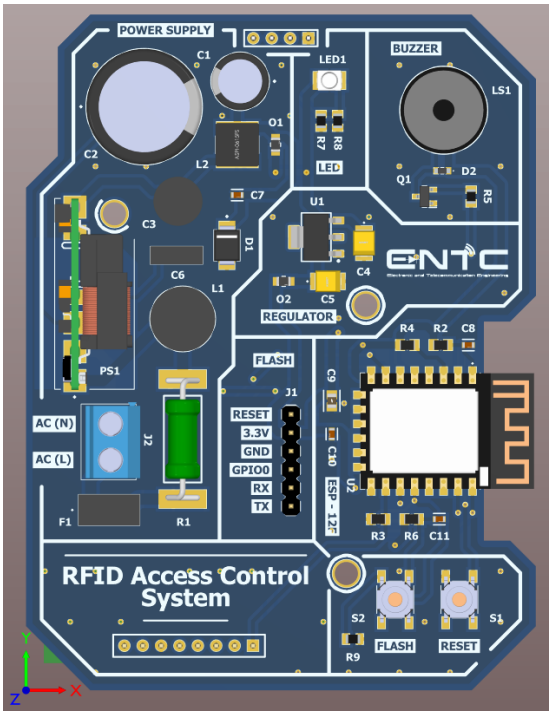


Figure 17: Top 3D view

9.9 Bottom 3D view

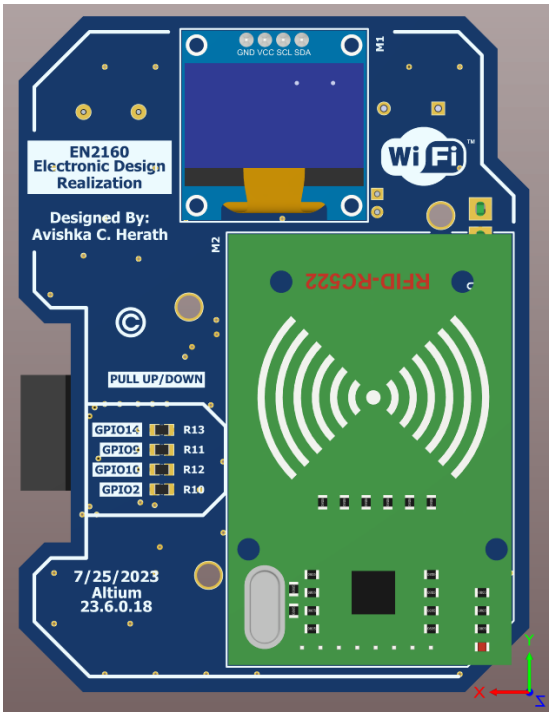


Figure 18: Bottom 3D view

9.10 3D isometric view

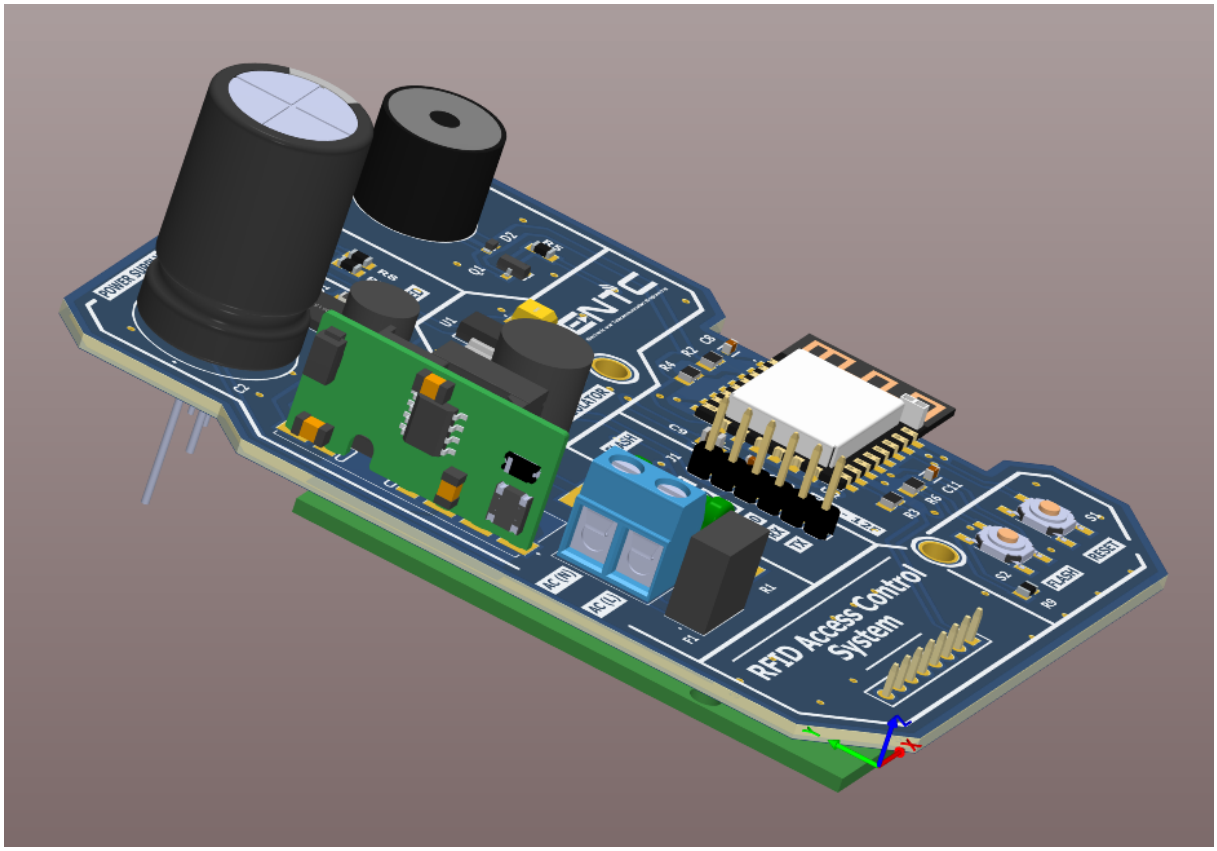


Figure 19: 3D isometric view

10 BOM

10.1 Mouser Electronics

Designator	Description	Quantity
PS1	AC/DC Power Modules ac-dc, 3 W, 5 Vdc, single output, open PCB	1
F1	Fuses with Leads - Through Hole 300V 1A SS-5H RADIAL TD FUSE	1
R1	Wirewound Resistors - Through Hole 3W 12 Ohms 5%	1
L1	Power Inductors - Leaded 1200uH 10% .48A	1
C5	Aluminum Electrolytic Capacitors - Radial Leaded 450volts 22uF 16x25 20% 7.5LS	1
C1	Aluminum Organic Polymer Capacitors 16Vol 270uF RAD 2KHr ESR=15 mOhms	1
L2	Power Inductors - SMD FIXED IND 4.7UH 2.2A 43 MOHM SMD	1
C4	Film Capacitors 0.001uF 630volts 5%	1
S1, S2	Tactile Switches 50mA 12VDC, 5.2x5.2mm, 1.5mm H, 160gf, G leads, No ground pin, metal actuator	2

C6, C7	Tantalum Capacitors - Solid SMD 10V 10uF 1311 20% ESR=3.5ohms	2
LS1	Piezo Buzzers & Audio Indicators buzzer, 12 mm x 9.5 mm deep, M, 3 V, 85 dB, Through Hole	1
P4	Fixed Terminal block, screw type, 5.00, horizontal, 2 poles, CUI Blue, slotted screw, PCB mount	1
D3	Standard LEDs - SMD WL-SMTW SMDMono TpVw Waterclr 3528 Blue	1

10.2 LCSC Electronics

Designator	Description	Quantity
C2	150uF 35V 130 mΩ@100kHz ±20% 640mA@100kHz Plugin,D8xL11.5mm Aluminum Electrolytic Capacitors - Leaded ROHS	5
C11	50V 100nF X7R ±5% 0603 Multilayer Ceramic Capacitors MLCC - SMD/SMT ROHS	100
C10	16V 10uF X5R ±10% 0805 Multilayer Ceramic Capacitors MLCC - SMD/SMT ROHS	50
D1	12V 7.78V 7V SMB(DO-214AA) TVS ROHS	5
R4, R5	125mW Thick Film Resistors ±100ppm/°C ±1% 330Ω 0805 Chip Resistor - Surface Mount ROHS	100
R6, R7	125mW Thick Film Resistors ±100ppm/°C ±1% 180Ω 0805 Chip Resistor - Surface Mount ROHS	100
U1	75dB@(120Hz) 800mA Fixed 3.3V~3.3V Positive 15V SOT-223 Linear Voltage Regulators (LDO) ROHS	1
Q1	30V 250mW 200@2mA,5V 100mA NPN SOT-23(TO-236) Bipolar Transistors - BJT ROHS	20
D2	30V Single 350mV@10mA 100mA SOD-523 Schottky Barrier Diodes (SBD) ROHS	20
R8, R9, R10, R11, R12, R13, R14, R15	125mW Thick Film Resistors ±100ppm/°C ±1% 10 kΩ 0805 Chip Resistor - Surface Mount ROHS	100
NA	Panel Mounting AC Power Receptacle -10°C ~+85°C 5A 250V Plugin AC/DC Power Connectors ROHS	1
R2, R3	125mW Thick Film Resistors 0Ω 0805 Chip Resistor - Surface Mount ROHS	100

10.3 Elecrow

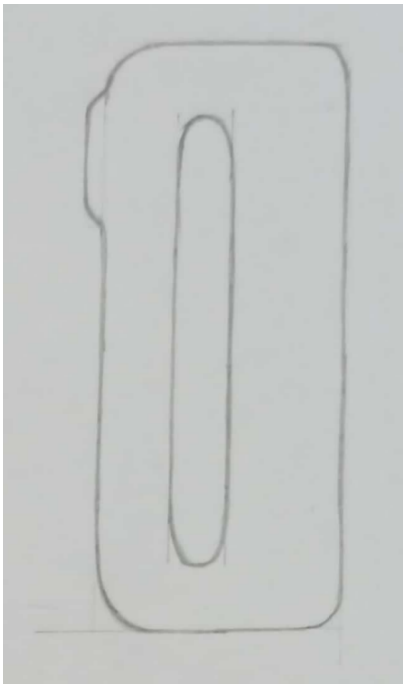
Designator	Description	Quantity
P1	RFID Reader with Cards Kit- 13.56MHz	1
P2	I2C 0.96" OLED 128x64- Blue	1
U2	ESP-12F Wi-Fi Module (ESP8266)	1
P3	40Pin 2.54mm Male Header - Black	1

11 Enclosure design

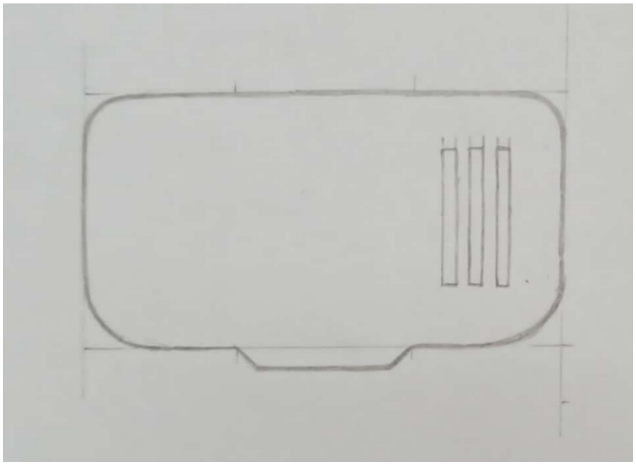
All enclosure designs were completed using Solidworks 2020 Student Edition.

11.1 Handsketches

(a) Top sketch



(b) Right sketch



(c) Front sketch

Figure 20: Handsketches

11.2 CAD designs

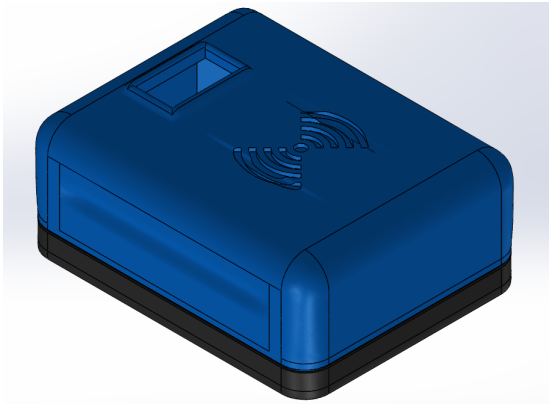


Figure 21: Enclosure top view

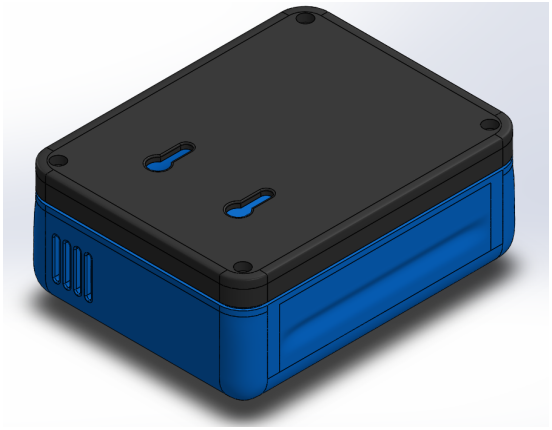


Figure 22: Enclosure bottom view

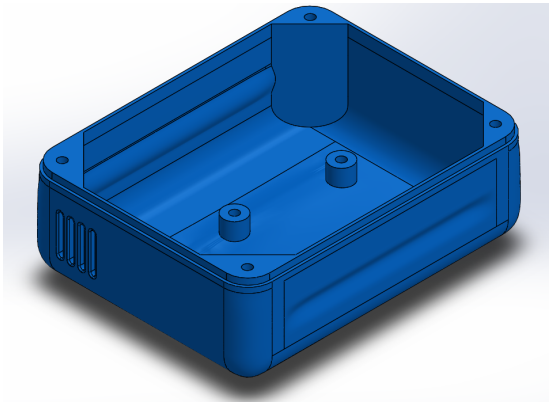


Figure 23: Base part inner surface

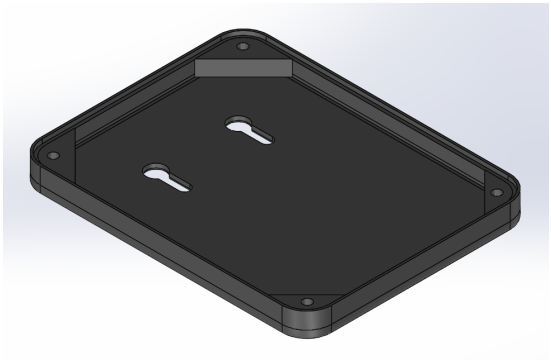


Figure 24: Cover part inner surface

11.3 Draft analysis and mold design

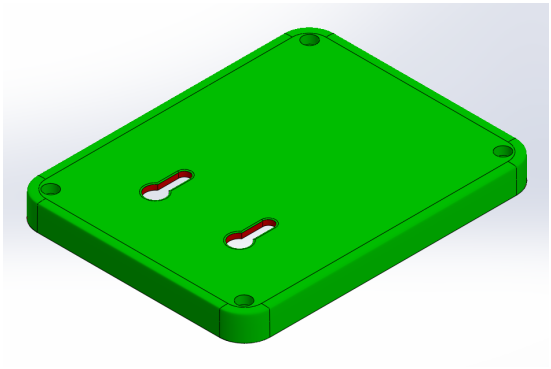


Figure 25: Draft analysis

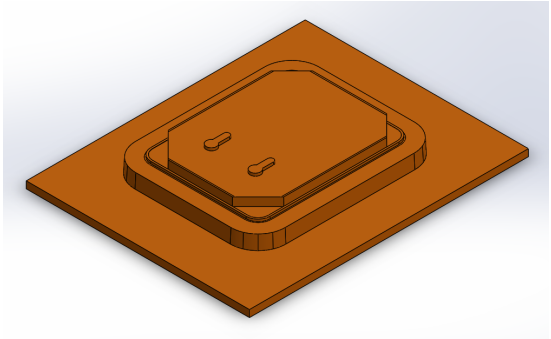


Figure 26: Mold design - Core

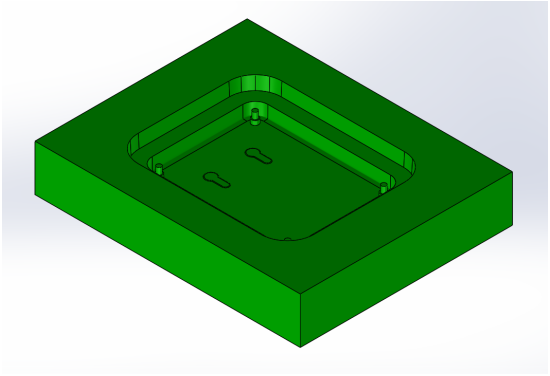


Figure 27: Mold design - Cavity

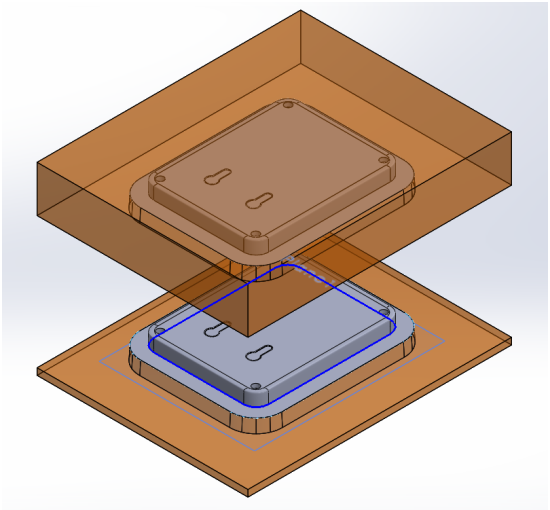


Figure 28: Core and Cavity

12 Web interface

12.1 Real time database

The integrated real-time database, powered by Firebase from Google, serves as the backbone of the RFID-Based Access Control and Smart Attendance System. Firebase offers a dynamic and scalable platform that enables seamless data storage, retrieval, and synchronization in real time. As users enter or exit the premises, their data is instantly updated and made available to the web user interface, providing administrators with real-time user status and attendance information. This dynamic database ensures that administrators have access to the latest data at all times, facilitating efficient access control management and accurate attendance tracking. The use of Firebase enhances the system's responsiveness and reliability, enabling administrators to make data-driven decisions and optimize facility operations effectively.

12.2 Web user interface

The web user interface of the RFID-Based Access Control and Smart Attendance System offers real-time user status, accessing data from a real-time database. It provides a comprehensive view of past entry/exit records, enabling administrators to monitor attendance trends and user movements. The user-friendly search option allows quick data retrieval based on the User ID. Additionally, administrators can effortlessly download records as CSV (Comma-Separated Values) files for further analysis and integration with other applications. With the added feature of visualizing user access locations, the interface empowers efficient access control management and attendance tracking, making it an essential tool for optimizing facility operations.

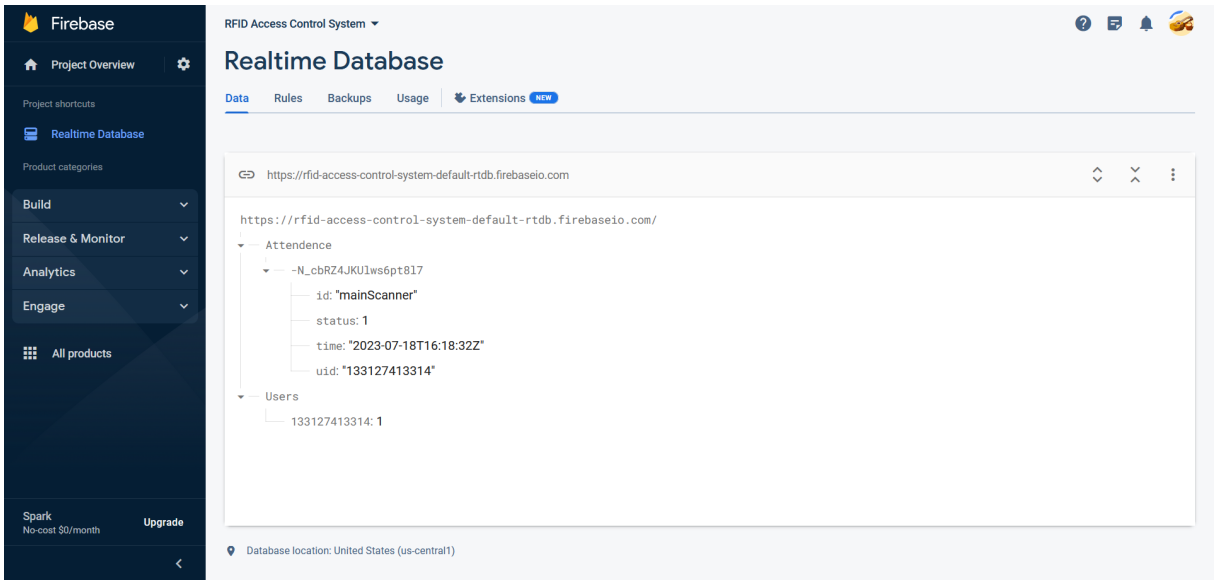


Figure 29: Real time database

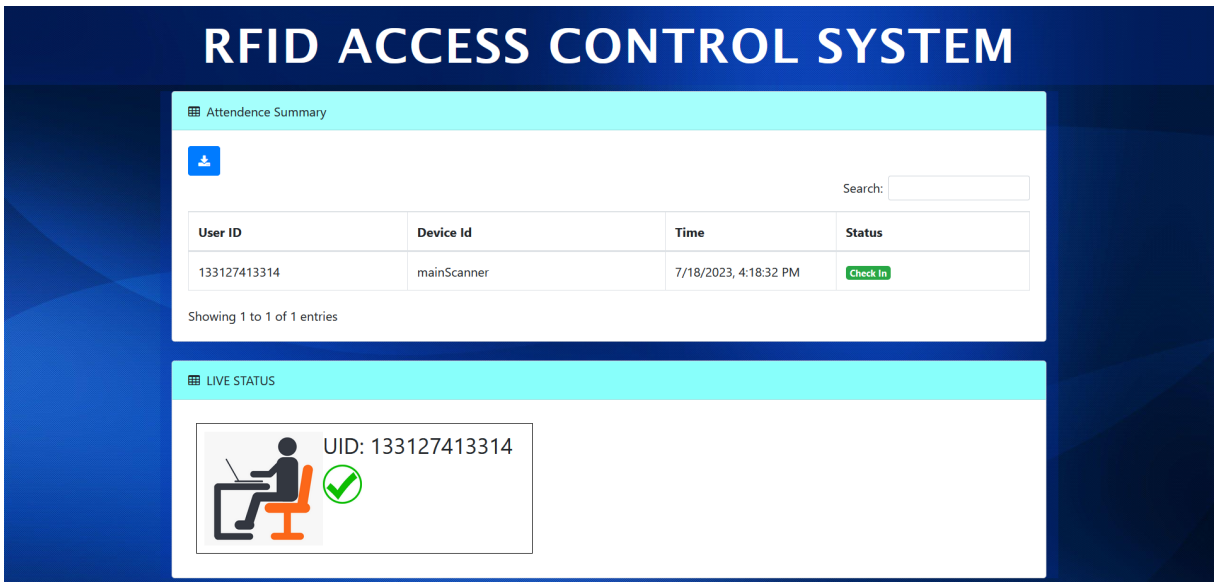


Figure 30: Web user interface

12.3 Features of the Web interface

The web user interface of the RFID-Based Access Control and Smart Attendance System offers the following key features:

- **Real-Time User Status**: Administrators can view the current status of users, including their access permissions and attendance data, in real-time.
- **Past Entry/Exit Records**: The interface provides a comprehensive view of historical entry and exit records, allowing administrators to monitor attendance trends and user movements over time.
- **Search Option**: Administrators can easily search for specific users or access records based on names, identification numbers, or other relevant criteria.
- **CSV Data Export**: Attendance records can be downloaded as CSV files, enabling seamless integration with other applications and facilitating further data analysis.

- **Displaying User Access Locations**: The interface displays the access points through which users enter or exit the facility, providing a visual representation of access patterns.

Overall, the web user interface's powerful features empower administrators with valuable insights and data-driven capabilities, making it an essential tool for optimizing facility operations and enhancing overall efficiency.

13 Software implementation

13.1 User initialization code

Registers new users in the database.

```
#include <ESP8266WiFi.h>
#include <SPI.h>
#include <Wire.h>
#include <RFID.h>
#include "FirebaseESP8266.h" // Firebase library
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>
#include <string.h>

#define FIREBASE_HOST "rfid-access-control-system-default-rtdb.firebaseio.com" //Without http:// or https:// schemes
#define FIREBASE_AUTH "LYSF6ajLypDTuY7zyUuTPM5ah4XU3z4sX3Do76z3"
RFID rfid(D8, D0);       //D8:pin of tag reader SDA. D0:pin of tag reader RST
unsigned char str[MAX_LEN]; //MAX_LEN is 16: size of the array

#define SCREEN_WIDTH 128 // OLED display width, in pixels
#define SCREEN_HEIGHT 64 // OLED display height, in pixels

// Declaration for an SSD1306 display connected to I2C (SDA, SCL pins)
#define OLED_RESET     -1 // Reset pin # (or -1 if sharing Arduino reset pin)
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);

const char ssid[] = "dusha123";
const char pass[] = "dushyantha";

int BUZZER = D3;

String uidPath= "/";
//Define FirebaseESP8266 data object
FirebaseData firebaseData;

void connect() {
  Serial.print("Checking WiFi...");
  OLEDprint("Checking WiFi...", 20, 10);
  while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(1000);
  }

  Serial.println("\n Connected!");
  blank();
```

```
  OLEDprint("Connected!", 20, 10);
  delay(1000);
  blank();
}

void blank(){
  display.clearDisplay();
  display.display();
 }

 void OLEDprint(String text,int row,int column){
  display.setTextSize(1);
  display.setTextColor(WHITE);
  display.setCursor(column, row);
  display.println(text);
  display.display();
 }

void setup()
{

  Serial.begin(115200);
  WiFi.begin(ssid, pass);
  pinMode(BUZZER, OUTPUT);

   // SSD1306_SWITCHCAPVCC = generate display voltage from 3.3V
   internally
  if(!display.begin(SSD1306_SWITCHCAPVCC, 0x3C)) {
    Serial.println(F("SSD1306 allocation failed"));
    for(;;); // Don't proceed, loop forever
  }

  blank();

  SPI.begin();
  rfid.init();

  connect();
  Firebase.begin(FIREBASE_HOST, FIREBASE_AUTH);
  Firebase.reconnectWiFi(true);
}
void pushUser (String temp)    //Function to check if an identified tag
   is registered to allow access
{
   Serial.println("PUSHING USER ID: "+temp);
    blank();
    OLEDprint("User ID:", 25, 10);
    OLEDprint(temp, 40, 10);
    digitalWrite (BUZZER, HIGH);
    delay(500);
    digitalWrite (BUZZER, LOW);
    Firebase.setInt(firebaseData, uidPath+"Users/"+temp,0);
    delay(500);
    blank();
}
void loop() {
  digitalWrite (BUZZER, LOW);
```

```
  OLEDprint("RFID Access Control", 25, 10);
  OLEDprint("System", 40, 50);
  if (rfid.findCard(PICC_REQIDL, str) == MI_OK)   //Wait for a tag to be placed near the reader
  {
    Serial.println("Card Found");
    blank();
    OLEDprint("Card Found", 20, 10);
    String temp = "";                             //Temporary variable to store the read RFID number
    if (rfid.anticoll(str) == MI_OK)              //Anti-collision detection, read tag serial number
    {
      Serial.print("The card's ID number is : ");
      for (int i = 0; i < 4; i++)                 //Record and display the tag serial number
      {
        temp = temp + (0x0F & (str[i] >> 4));
        temp = temp + (0x0F & str[i]);
      }
      delay(200);
      blank();
      Serial.println (temp);
      pushUser (temp);     //Check if the identified tag is an allowed to open tag
    }
    rfid.selectTag(str); //Lock card to prevent a redundant read, removing the line will make the sketch read cards continually
  }
  rfid.halt();
}
```

13.2 Main device code for Access control

```
#include <ESP8266WiFi.h>
#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>
#include <string.h>
#include <SPI.h>
#include <RFID.h>
#include "FirebaseESP8266.h"  // Install Firebase ESP8266 library
#include <NTPClient.h>
#include <WiFiUdp.h>

#define FIREBASE_HOST "rfid-access-control-system-default-rtdb.firebaseio.com" //Without http:// or https:// schemes
#define FIREBASE_AUTH "LYSF6ajLypDTuY7zyUuTPM5ah4XU3z4sX3Do76z3"

RFID rfid(D8, D0);       //D10:pin of tag reader SDA. D9:pin of tag reader RST
unsigned char str[MAX_LEN]; //MAX_LEN is 16: size of the array

#define SCREEN_WIDTH 128 // OLED display width, in pixels
#define SCREEN_HEIGHT 64 // OLED display height, in pixels

```

```
// Declaration for an SSD1306 display connected to I2C (SDA, SCL pins)
#define OLED_RESET     -1 // Reset pin # (or -1 if sharing Arduino reset pin)
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);

WiFiUDP ntpUDP;
const long utcOffsetInSeconds = 19800; //(UTC+5:30)
NTPClient timeClient(ntpUDP, "pool.ntp.org");

const char ssid[] = "Avishka Redmi";
const char pass[] = "avishkacherath";

int BUZZER = D3;

String uidPath= "/";
FirebaseJson json;

FirebaseData firebaseData;  //Define FirebaseESP8266 data object

unsigned long lastMillis = 0;
String alertMsg;
String device_id="mainScanner";
boolean checkIn = true;

void connect() {
  Serial.print("Checking WiFi ...");
  OLEDprint("Checking WiFi ...", 30, 10);
  while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(1000);
  }

  Serial.println("\n Connected!");
  blank();
  OLEDprint("Connected!", 30, 35);
  delay(1000);
  blank();
}

void blank(){
  display.clearDisplay();
  display.display();
 }

 void OLEDprint(String text,int row,int column){
  display.setTextSize(1);
  display.setTextColor(WHITE);
  display.setCursor(column, row);
  display.println(text);
  display.display();
 }

void setup()
{

  Serial.begin(115200);
```

```
  WiFi.begin(ssid, pass);

  pinMode(BUZZER, OUTPUT);

   // SSD1306_SWITCHCAPVCC = generate display voltage from 3.3V internally
  if(!display.begin(SSD1306_SWITCHCAPVCC, 0x3C)) {
    Serial.println(F("SSD1306 allocation failed"));
    for(;;); // Don't proceed, loop forever
  }

  blank();

  SPI.begin();
  rfid.init();

  timeClient.begin();
  timeClient.setTimeOffset(utcOffsetInSeconds);
  connect();
  Firebase.begin(FIREBASE_HOST, FIREBASE_AUTH);
  Firebase.reconnectWiFi(true);
}
void checkAccess (String temp)    //Function to check if an identified tag is registered to allow access
{
    if(Firebase.getInt(firebaseData, uidPath+"/Users/"+temp)){

      if (firebaseData.intData() == 0)          //If firebaseData.intData() == checkIn
      {
           alertMsg="CHECKING IN";
           blank();
           OLEDprint("User ID :", 10, 10);
           OLEDprint(temp, 25, 30);
           OLEDprint("ACCESS GRANTED", 45, 20);

           digitalWrite (BUZZER, HIGH);
           delay(1000);
           digitalWrite (BUZZER, LOW);

           blank();
           OLEDprint("Checking IN", 30, 30);

           json.add("time", String(timeClient.getFormattedDate()));
           json.add("id", device_id);
           json.add("uid", temp);
           json.add("status",1);

           Firebase.setInt(firebaseData, uidPath+"/Users/"+temp,1);

           if (Firebase.pushJSON(firebaseData, uidPath+ "/Attendence", json)) {
             Serial.println(firebaseData.dataPath() + firebaseData.pushName());
           } else {
             Serial.println(firebaseData.errorReason());
           }
```

```
128             blank();
129       }
130       else if (firebaseData.intData() == 1)    //If the lock is open then
      close it
131       {
132             alertMsg="CHECKING OUT";
133             blank();
134             OLEDprint("User ID :", 10, 10);
135             OLEDprint(temp, 25, 30);
136             OLEDprint("ACCESS GRANTED", 45, 20);
137
138             digitalWrite (BUZZER, HIGH);
139             delay(1000);
140             digitalWrite (BUZZER, LOW);
141
142             blank();
143             OLEDprint("Checking OUT", 30, 30);
144
145             Firebase.setInt(firebaseData, uidPath+"/Users/"+temp,0);
146
147             json.add("time", String(timeClient.getFormattedDate()));
148             json.add("id", device_id);
149             json.add("uid", temp);
150             json.add("status",0);
151
152             if (Firebase.pushJSON(firebaseData, uidPath+ "/Attendence",
     json)) {
153               Serial.println(firebaseData.dataPath() + firebaseData.
     pushName());
154             } else {
155               Serial.println(firebaseData.errorReason());
156             }
157             blank();
158       }
159     }
160     else
161     {
162       Serial.println("FAILED");
163
164       blank();
165       OLEDprint("User ID :", 10, 10);
166       OLEDprint(temp, 25, 30);
167       OLEDprint("ACCESS DENIED", 45, 20);
168
169       digitalWrite (BUZZER, HIGH);
170       delay(300);
171       digitalWrite (BUZZER, LOW);
172       delay(100);
173       digitalWrite (BUZZER, HIGH);
174       delay(500);
175       digitalWrite (BUZZER, LOW);
176
177       Serial.println("REASON: " + firebaseData.errorReason());
178       blank();
179     }
180 }
181 void loop() {
```

```
  digitalWrite (BUZZER, LOW);

  OLEDprint("RFID Access Control", 10, 10);
  OLEDprint("System", 25, 50);
  OLEDprint("- Place ID to scan -", 50, 5);

  timeClient.update();
  if (rfid.findCard(PICC_REQIDL, str) == MI_OK)   //Wait for a tag to be placed near the reader
  {
    Serial.println("Card found");
    blank();
    OLEDprint("Scanning ...", 25, 30);

    String temp = "";                             //Temporary variable to store the read RFID number
    if (rfid.anticoll(str) == MI_OK)              //Anti-collision detection, read tag serial number
    {
      Serial.print("The card's ID number is : ");
      for (int i = 0; i < 4; i++)                 //Record and display the tag serial number
      {
        temp = temp + (0x0F & (str[i] >> 4));
        temp = temp + (0x0F & str[i]);
      }
      Serial.println (temp);
      checkAccess (temp);     //Check if the identified tag is an allowed to open tag
    }
    rfid.selectTag(str); //Lock card to prevent a redundant read, removing the line will make the sketch read cards continually
  }
  rfid.halt();
}
```

13.3 Webpage

The HTML code for the webpage.

```
<!DOCTYPE html>
<html lang="en">

<head>
  <title>RFID-Access-Control</title>
  <meta charset="UTF-8">
<!-- Below is the initialization snippet for my Firebase project. It will vary for each project -->

<script src="https://www.gstatic.com/firebasejs/5.5.5/firebase.js"></script>
<script>
  // Initialize Firebase
  var config = {
    apiKey: "AIzaSyAPCXkitM_3dI-crYU3EI7YNgMGjJkL4LY",
    authDomain: "rfid-access-control-system.firebaseapp.com",
```

```
    databaseURL: "https://rfid-access-control-system-default-rtdb.firebaseio.com",
    projectId: "rfid-access-control-system",
    storageBucket: "rfid-access-control-system.appspot.com",
    messagingSenderId: "866858418543",
    appId: "1:866858418543:web:d9ede3a9f19be0c47e289a",
    measurementId: "G-98LW2FJ15E"

  };
  firebase.initializeApp(config);
</script>
<link href="style.css" rel="stylesheet">
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap.min.css">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link href="https://cdn.datatables.net/1.10.20/css/dataTables.bootstrap4.min.css" rel="stylesheet" crossorigin="anonymous"/>
<link href="https://cdn.datatables.net/responsive/2.2.6/css/responsive.dataTables.min.css" rel="stylesheet">
</head>
<body>
    <div class="heading">
        <h1 style="font-family: 'Lucida Sans', 'Lucida Sans Regular', 'Lucida Grande', 'Lucida Sans Unicode', Geneva, Verdana, sans-serif;">RFID ACCESS CONTROL SYSTEM</h1>
    </div>
  <div style="background-color: #062bb13f;" class="container">
    <div class="card">
      <div style="background-color: rgba(0, 255, 247, 0.352);" class="card-header">
          <i class="fa fa-table mr-1"></i>
          Attendence Summary
      </div>
      <div class="card-body">
        <button type="button" class="btn btn-primary" id="export">
          <i class="fa fa-download" aria-hidden="true"></i>
        </button>
          <div class="table-responsive">
              <table class="table table-bordered display responsive nowrap" id="buttonTable" width="100%" cellspacing="0" data-order="[]">
                  <thead>
                      <tr>
                          <th>User ID</th>
                          <th>Device Id</th>
                          <th>Time</th>
                          <th>Status</th>
                      </tr>
                  </thead>
                  <tbody>

                  </tbody>
              </table>
          </div>
      </div>
  </div>
```

```
  <div class="card mt-4">
      <div style="background-color: rgba(0, 255, 247, 0.467);" class="
    card-header">
          <i class="fa fa-table mr-1"></i>
          LIVE STATUS
      </div>
      <div class="card-body Users">

      </div>
  </div>
  </div>

  <script src="https://code.jquery.com/jquery-3.1.1.min.js"></script>
  <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/
    bootstrap.min.js"></script>
  <script src="https://cdn.datatables.net/1.10.20/js/jquery.dataTables.
    min.js" crossorigin="anonymous"></script>
  <script src="https://cdn.datatables.net/1.10.20/js/dataTables.
    bootstrap4.min.js" crossorigin="anonymous"></script>
  <script src="https://cdn.datatables.net/responsive/2.2.6/js/dataTables
    .responsive.min.js"></script>
  <script src="https://cdn.datatables.net/buttons/1.5.2/js/dataTables.
    buttons.min.js"></script>
<script src="https://cdn.datatables.net/buttons/1.5.2/js/buttons.flash.
    min.js"></script>
<script src="https://cdn.datatables.net/buttons/1.5.2/js/buttons.html5.
    min.js"></script>
<script src="https://cdn.datatables.net/buttons/1.5.2/js/buttons.print.
    min.js"></script>

  <script>
    $(function(){
      $('.Users').html('No data available');
      document.getElementById("export").onclick = function() { exportCSV
    () };

      function exportCSV() {
      //// export CSV
        console.log("exportCSV");
        $('#buttonTable').DataTable().button(0).trigger();
      }

      var button_table = $('#buttonTable').DataTable({
        "ordering": false,
        "paging": false,
        buttons: [
          {
            extend: 'csv',
            filename: 'file_name',
            extension: '.csv'
          }
        ],
        initComplete: function() {

        $('.buttons-csv').hide();
      }
    });
```

```
109
110     firebase.database().ref('/').on('value',function(snap){
111       if(snap.val().Users){
112         let obj= snap.val().Users;
113         console.log(obj);
114         $('.Users').html('');
115         if(Object.keys(obj).length>0){
116           Object.keys(obj).forEach(key=>{
117             $('.Users').append(`
118             <div class="live">
119               <img src="./img/checkin.png" width="150px">
120               <ul>
121                 <li><h3>UID: ${key}</h3></li>
122                 <li><img id="true${key}" width="50px" src="./img/tick.
    png"></li>
123                 <li><img id="false${key}" width="50px" src="./img/cross.
    png"></li>
124               </ul>
125             </div>
126             `);
127             if(obj[key]==1){
128               $('#true'+key).show();
129               $('#false'+key).hide();
130             }else{
131               $('#true'+key).hide();
132               $('#false'+key).show();
133             }
134           })
135         }
136       }
137       if(snap.val().Attendence){
138           button_table.clear().draw();
139
140           let arr= Object.values(snap.val().Attendence);
141           console.log(arr);
142           arr.forEach(function(elem,i){
143               //console.log(table.row);
144               var row= `<tr>
145                   <td>${elem.uid}</td>
146                   <td>${elem.id}</td>
147                   <td>${new Date(elem.time.slice(0, -1)).toLocaleString
    ()}</td>
148                   <td id="state${new Date(elem.time).getTime()}"></td>
149               </tr>`;
150               button_table.rows.add($(row)).draw();
151               if(elem.status){
152                   //console.log(elem.status);
153                   $('#state'+new Date(elem.time).getTime()).html('<span
    class="badge badge-success">Check In</span>');
154               }else{
155                   $('#state'+new Date(elem.time).getTime()).html('<span
    class="badge badge-danger">Check Out</span>');
156               }
157           })
158       }
159     })
160
```

```
});
  </script>
</body>

</html>
```

The CSS code for the webpage.

```
.heading h1{
    text-align: center;
    font-size: 60px;
    letter-spacing: 3px;
    background: #062bb13f;
    font-family: 'Courier New', Courier, monospace;
    color: white;
}

body {
  background-image: url('background image2.jpg');
  background-repeat: no-repeat;
  background-size: cover;
}

@media only screen and (max-width: 600px) {
    .heading h1{
      font-size: 20px;
  }
}
.heading{
  position: relative;
}
.heading i{
  position: absolute;
  left: 90%;
  top: 14%;
}
ul{
    padding: 0;
    margin: 0;
    list-style: none;
}
.live{
    border: 1px solid black;
    width: 40%;
    margin: 10px;
    padding: 10px;
    float: left;
}
.live img{
    float: left;
}
.parkings{
    border: 1px solid black;
    width: 100%;
    margin: 10px;
    padding: 10px;
}
```

```
.bookContainer{
    border: 1px solid black;
    width: 40%;
    margin: 10px;
    padding: 10px;
    float: left;
}

.show{
    display: block;
}


/* The switch - the box around the slider */
.switch {
    position: relative;
    display: inline-block;
    width: 60px;
    height: 34px;
  }

  /* Hide default HTML checkbox */
  .switch input {
    opacity: 0;
    width: 0;
    height: 0;
  }

  /* The slider */
  .slider {
    position: absolute;
    cursor: pointer;
    top: 0;
    left: 0;
    right: 0;
    bottom: 0;
    background-color: #ccc;
    -webkit-transition: .4s;
    transition: .4s;
  }

  .slider:before {
    position: absolute;
    content: "";
    height: 26px;
    width: 26px;
    left: 4px;
    bottom: 4px;
    background-color: white;
    -webkit-transition: .4s;
    transition: .4s;
  }

  input:checked + .slider {
    background-color: #2196F3;
  }

```

```
  input:focus + .slider {
    box-shadow: 0 0 1px #2196F3;
  }

  input:checked + .slider:before {
    -webkit-transform: translateX(26px);
    -ms-transform: translateX(26px);
    transform: translateX(26px);
  }

  /* Rounded sliders */
  .slider.round {
    border-radius: 34px;
  }

  .slider.round:before {
    border-radius: 50%;
  }

  #form{
    position: relative;
  }
  #heading2{
    position: absolute;
    top: 50%;
  }

.modal-header, h4, .close {
    background-color: #5cb85c;
    color:white !important;
    text-align: center;
    font-size: 30px;
}
.modal-footer {
    background-color: #f9f9f9;
}
@media (min-width:767px){
  #contain{
      padding-top: 20px;
      width: 40%;
  }
}
.page{
  height:560px;
  overflow-y: scroll;
}
.heading h1 {
  color: #ffffff;
  line-height: 60px;
  font-weight: bold;
  font-family: 'Aldrich';
  font-size: 60px;
  letter-spacing: 2px;
  text-align: center;
  text-transform: uppercase;
  margin-top: 0px;
  padding-top:20px;
```

```
  padding-bottom: 20px;
}
```

14 Cost of the product

Description	Amount ($)
Mouser component expenses (+ shipping)	13.89
LCSC component expenses (+ shipping)	7.81
Elecrow component expenses (+ shipping)	11.69
PCB - JLC (+ shipping)	5.65
3D printed enclosure	20.05
Other expenses	5.00
Total expenses	**64.09**

Therefore the total cost for the product is around LKR 21025.21

Part III
Manufacturing planning and preparation

The subsequent sections will cover the processes of PCB fabrication, soldering, testing, and enclosure manufacturing.

15 PCB Manufacturing

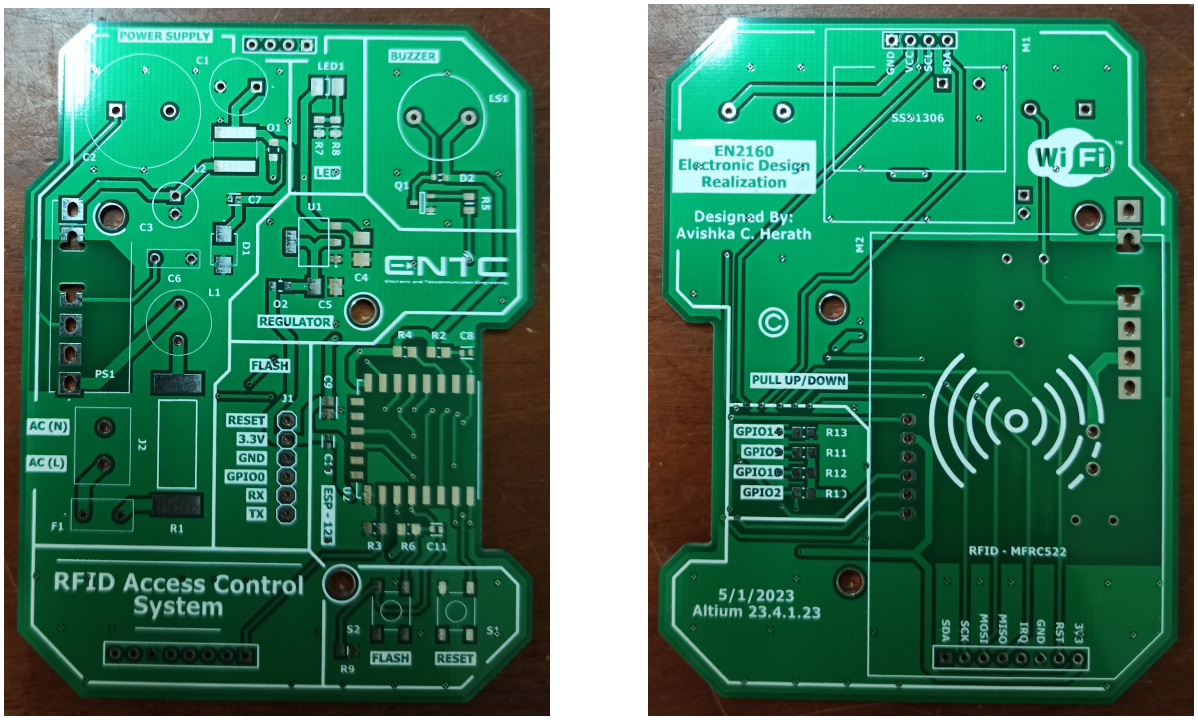
The PCB was designed using Altium 23.4. The bill of materials for the PCB is attached in this document. The PCB is double-sided (2 layers), with components placed on both the top and bottom layers. Due to the lack of local facilities for manufacturing PCBs, the PCB manufacturing is outsourced to a Chinese company.

PCB Manufacturer - Jia Li Chuang (Hong Kong) Co., Limited (JLC PCB)

15.1 PCB specifications

- Layers: 2
- Board thickness: 1.6mm
- Surface finish: HASL (with lead)
- Copper Weight: 1 oz
- Material Type: FR4-Standard Tg 130-140C

The required Gerber Files can be found in the following link: https://github.com/avishkaherath/RFID-Access-Control-System



(a) Top PCB (b) Bottom PCB

Figure 31: Manufactured PCB from JLC PCB

16 Soldering

16.1 Safety precautions

- The soldering process should only be performed by qualified technicians who have received proper training.
- Ensure that the workstation is clean and dry.
- Always wear protective gear to avoid inhaling fumes.
- Handle ICs (Integrated Circuits) with care, avoiding direct contact with bare hands to prevent potential damage from electrostatic discharge. Utilize a conducting wristband and grounding mat to safely discharge any accumulated charge to the ground.
- Practice precise temperature control during soldering, and consult the datasheets of components to understand their temperature sensitivity and prevent any potential damage.
- Dispose of used solder sponges and contaminated rags in a sealable bag as hazardous waste.
- Adhere to standard safety practices throughout the soldering process.

16.2 PCB Soldering

For the assembly of both through-hole and SMD components, it is advisable to follow the hand soldering technique. Hand soldering is preferred due to the smaller number of components, leading to reduced costs and fewer chances of soldering errors. Here are the instructions for component preparation and soldering equipment:

- Ensure the components' tips are cleaned to eliminate any oxide layer by brushing them and washing them with a solution of 99% isopropyl alcohol.
- Apply Rosin flux to the surfaces to be soldered, as it aids in removing any oxidized metal.

- To ensure the safety of components, use a 30W soldering iron (40W maximum).
- For the soldering iron, it is recommended to use a Conical or B-series tip.
- Utilize 20 AWG (0.813mm) 60/40 soldering wire for the soldering process.
- Start the soldering process with smaller, low-temperature sensitive components before moving on to larger, high-temperature sensitive ones.
- Exercise caution when soldering the ESP-12F module to avoid subjecting it to continuous high temperatures, as this can cause damage to its internal structure.

Figure 32: Conical or B-series tip

Note - The OLED display is connected to the PCB using a 4-pin JST connector. Therefore, position the connector on the PCB from the Top layer and apply solder from the bottom. Also, solder the 4 wires of the JST to the OLED in the correct order.

- Solder a 14 AWG wire, 8 cm in length, to the AC panel mount connector's terminals as shown in the figure below. Use Brown and Blue wires to indicate the Live and Neutral wires of the AC power line, respectively. Additionally, add heat shrink tubing to the soldered end to ensure proper electrical safety.

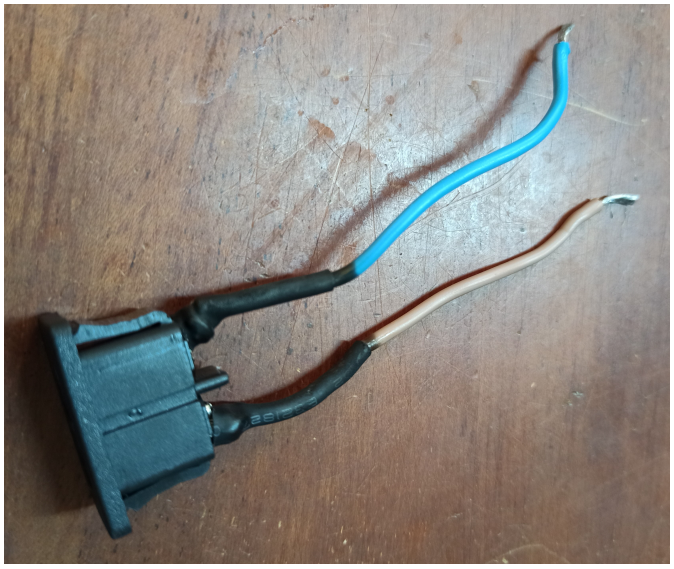
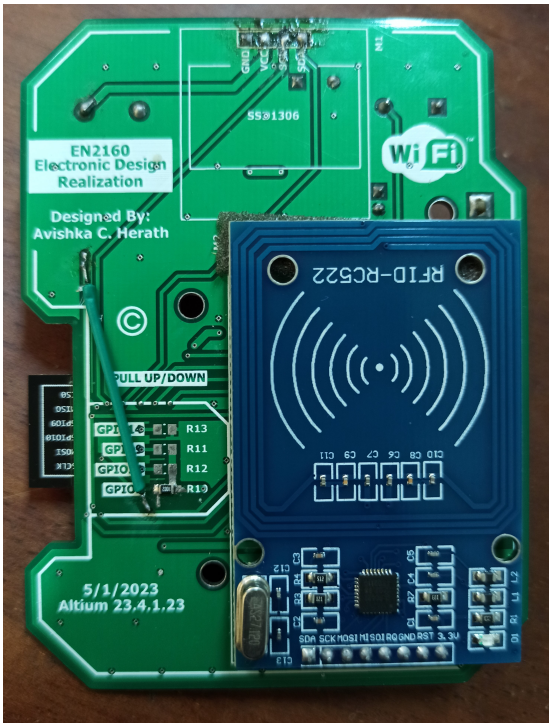


Figure 33: Panel Mounting AC Power Receptacle Connections

(a) Soldered PCB - Top



(b) Soldered PCB - Bottom

Figure 34: Final soldered PCB

17 PCB Testing

PCBs are designed with test points, and the PCB in question consists of three separate blocks, each independent of the others. Testing procedures can be conducted separately for each block, verifying their functionality individually. Once the functionality of each block is confirmed, they can be interconnected using 0 Ω resistors in a cascading manner.
Test the PCB in the following order:

1. Power supply block
2. Regulator block
3. Micro-controller block

17.1 Power supply block

To perform the test:

1. Connect the COM (common) probe of the multimeter to the GND (Ground) pin of the PCB.
2. Place the other probe on test point 1 (O_1) and check whether the multimeter reads +5V.
3. Keep in mind that the +5V net is directly connected to the power LED, so it may light up when the PCB is powered ON.

By following these steps, you can measure and verify the voltage at test point 1 on the PCB. Ensure proper safety measures and caution while working with electrical components and power sources.

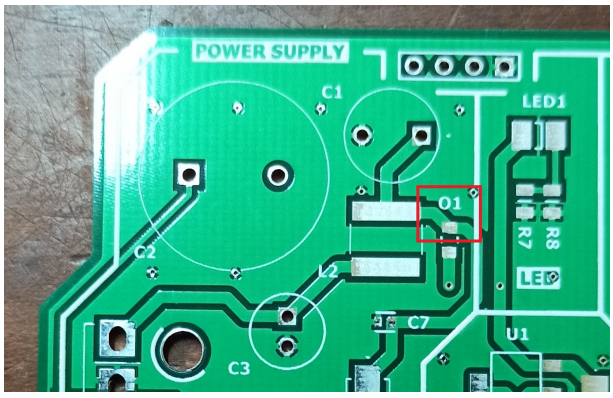


Figure 35: Testing the output voltage of power supply

17.2 Regulator block

To perform the test:

1. Connect the COM (common) probe of the multimeter to the GND (Ground) pin of the PCB.
2. Place the other probe on test point 2 (O_2) and check whether the multimeter reads +3.3V.
3. Keep in mind that the +3.3V net is directly connected to the power LED, so it may light up when the PCB is powered ON.

By following these steps, you can measure and verify the voltage at test point 2 on the PCB.

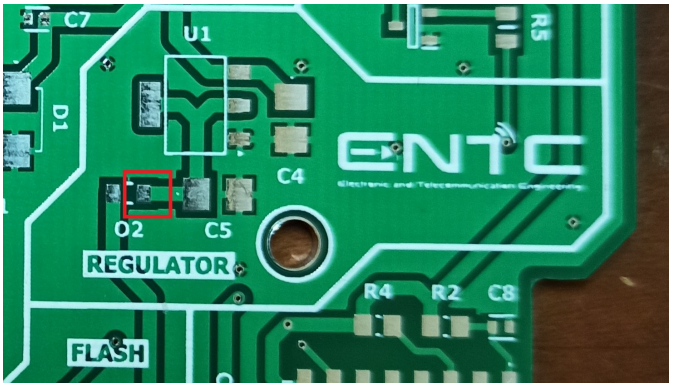


Figure 36: Testing the output voltage of +3.3V regulator

17.3 Micro-controller block

To perform the test:

1. Check the connectivity of the block using the multimeter in Connectivity Mode.
2. Connect +3.3V pin and GND pin to a +VCC and GND of a +3.3V power supply and check whether the LED of the ESP-12F light up.
3. Check the voltages of each pull-up/down resistor.
4. Upload a code to make the digital output of the GPIO2 (D4) pin HIGH and LOW, each with a delay.

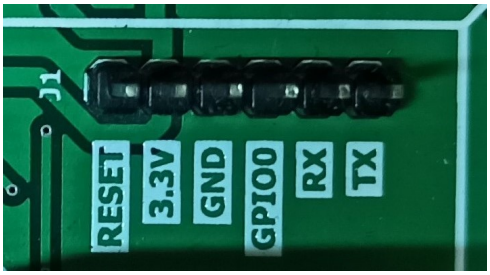
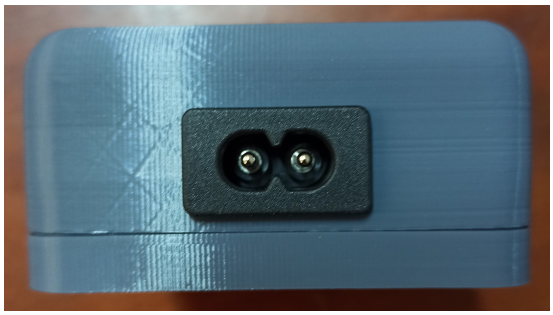


Figure 37: Testing the micro-controller connections

(a) Top view

(b) Bottom view



(c) Rear view

(d) Front view

Figure 38: Manufactured enclosure

18 Enclosure Manufacturing

Enclosure was manufactured using 3D printing. The selected specifications for manufacturing the enclosure are listed below.

- Material: PLA+
- Layer height: 0.2mm
- Infill rate: 20%

Figure 39: Final view of the design

19 Uploading the code

19.1 Setting up the connections

You can use an ESP8266 Development Board (NodeMCU) or an USB to TTL converter to upload the code. To program the ESP-12F module set up the connections as follows:

- Connect the +3.3V to +3.3V of the NodeMCU or a suitable power supply.
- Connect the GND to GND pin of the NodeMCU or a suitable power supply.
- Connect the RST pin to the RESET pins of the NodeMCU (This connection is not needed when using the USB to TTL converter).
- Connect TX, RX to the TX and RX pins respectively. (Interchange the connections if you are using a USB to TTL converter)
- Connect GPIO2 pin of the module to the pin D4 of the NodeMCU (This connection is not needed when using the USB to TTL converter).

Now the code is ready to be uploaded to the micro-controller using the Arduino IDE.

19.2 Setting up the programmer

The Arduino IDE is used to upload the code. Set the initial setup of the IDE as follows:
Now upload the final code to the micro-controller.

Figure 40: Setting up the connections and uploading the code

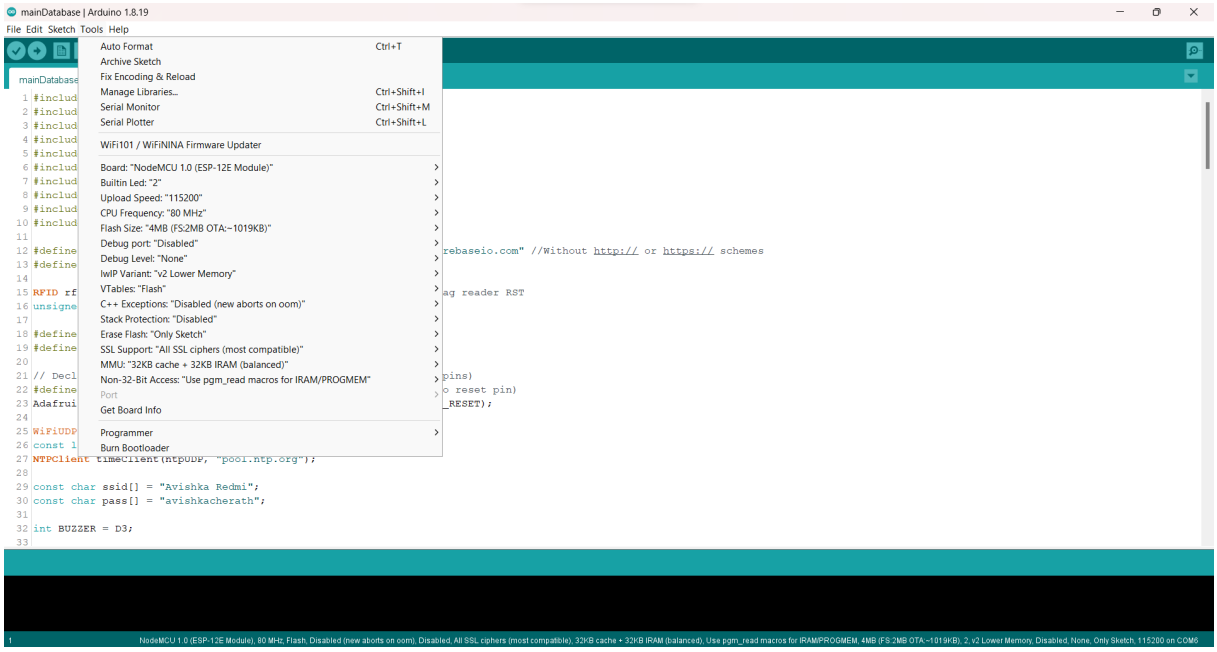


Figure 41: Setting up the programmer settings

20 Assembly

Follow the steps below to assemble the separate parts:

1. **Secure the OLED to the enclosure** using four 2mm (M2) self-tapping screws. Ensure the OLED is properly aligned, and then tighten the screws to hold it firmly in place.

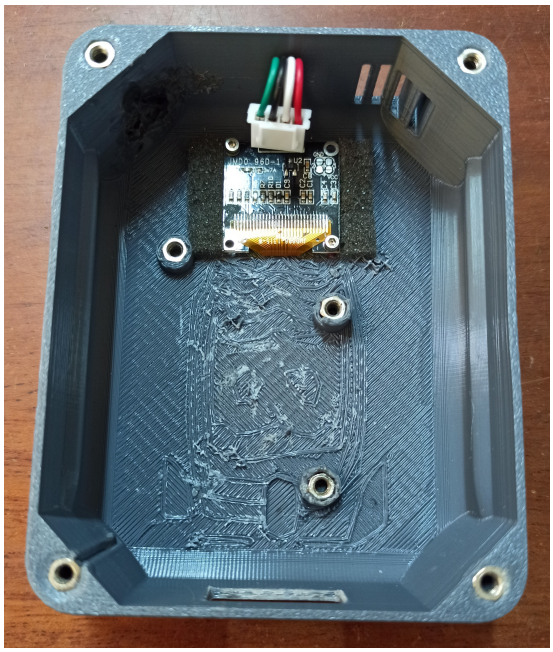


Figure 42: Mounting of the OLED display

2. **Connect the AC power line to the terminal blocks** and tighten the connections. Ensure that the wires of the AC power are routed through the appropriate mounting hole.
3. **Place the PCB inside the enclosure**, making sure all components and connectors are correctly aligned with the designated slots and openings.
4. **Connect the OLED JST connector** and mount the AC power connector to the enclosure.
5. **Mount the PCB to the enclosure** using three screws after ensuring proper alignment.

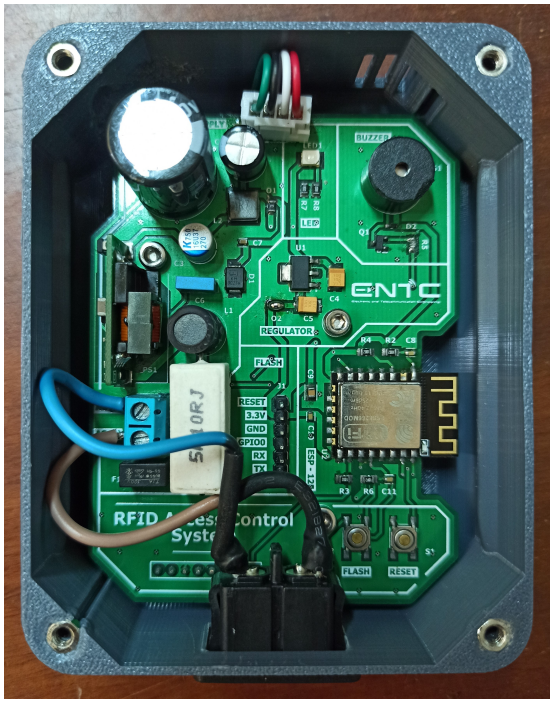


Figure 43: Fully assembled product inside view

6. **Close the top cover** and secure it in place using four screws. The screws used for mounting the PCB and top cover to the enclosure are M3 Allen Nuts.

By following these steps, you will have successfully assembled the separate parts into the enclosure. Ensure that all connections are secure, and refer to any specific assembly instructions or documentation provided for your project. Always exercise caution and follow safety guidelines when working with electrical components and power sources.

Figure 44: Finally assembled design

21 Product specifications

- Input Voltage: 230V AC / 50Hz
- Operating Voltage: +3.3V / +5V
- Maximum Power: 3W
- RFID Operating Frequency: 13.56 MHz
- RFID Typical Operating Distance: 50 mm
- Display: 128 $\times$ 64 OLED Display
- Minimum Buzzer Sound Pressure Level: -85 dB
- Operating Ambient Temperature: -25 °C to +70 °C
- Wi-Fi Connectivity: Wi-Fi 2.4 GHz, support WPA/WPA2
- Enclosure Material: PLA+
- Product Dimensions: 100 x 80 x 40 mm

Part IV
Future developments and acknowledgment

22 Future development

The future development of the RFID-based access control system envisions a significant advancement in security and efficiency, leveraging emerging technologies to optimize its capabilities. One crucial area of development involves the integration of multi-factor authentication, combining RFID technology with other biometric methods such as fingerprint, facial recognition, or iris scanning. This multi-layered approach will bolster security, ensuring more accurate user identification and reducing the risk of unauthorized access.

Furthermore, the system will embrace artificial intelligence (AI) to continuously improve its performance. AI algorithms will analyze access patterns, detect anomalies, and predict potential security threats in real-time, enabling proactive response mechanisms and enhancing overall system intelligence.

Cloud-based infrastructure will be a pivotal aspect of future developments, allowing for a centralized and scalable system. Cloud integration will enable seamless data synchronization across multiple access points, real-time updates, and remote management capabilities, providing a more agile and user-friendly system.

The evolution of the RFID-based access control system will also involve mobile access options, enabling employees to use their smartphones as virtual access tokens. This contactless approach will enhance user convenience while maintaining security standards. Administrators will have remote access to manage access permissions, view access logs, and receive real-time alerts, facilitating efficient system management from any location.

To fortify data integrity and enhance auditability, the system will explore the implementation of blockchain technology. Storing access control data in a distributed ledger will create an immutable and transparent record of access events, bolstering trust and accountability.

Energy efficiency will be a key consideration in future developments. The system will optimize power consumption of RFID devices and explore renewable energy sources to minimize environmental impact, promoting sustainability in its operations.

Overall, the future development of the RFID-based access control system promises an intelligent, secure, and user-centric solution. By integrating multi-factor authentication, AI, cloud-based infrastructure, mobile access, blockchain, and energy-efficient measures, the system will set new standards in access control technology, meeting the evolving needs of organizations in the digital age.

23 Acknowledgment

We express our sincere gratitude and appreciation to all those who have played a vital role in the development of this remarkable marketable product. Without the combined efforts and dedication of these exceptional individuals and teams, this design document would not have been successfully realized.

First and foremost, we extend our heartfelt thanks to our lecturers for their unwavering support and encouragement throughout this project. Their strategic guidance and commitment to innovation have been invaluable in shaping the concept and driving us towards excellence.

We also wish to acknowledge the dedication of our departmental friends, who diligently tested and paid meticulous attention to detail, ensuring our product adheres to the highest standards of performance and reliability.

A special acknowledgment goes to Mr. Sameera, our esteemed Analog laboratory Technical Officer, and Mr. Chaminda, our dedicated Analog laboratory assistant. Their collaboration and commitment played a pivotal role in overcoming challenges and achieving excellence in product development. Their support in providing essential measuring equipment and assisting in circuit fabrication have been instrumental in our achievements.

Lastly, our heartfelt appreciation goes to our customers, whose valuable feedback and unwavering support have been the driving force behind our pursuit of excellence. Their trust in our product motivates us to continuously improve and optimize our offerings.

In conclusion, this marketable product is a testament to the power of teamwork, determination, and innovation. Together, we have surmounted hurdles, embraced challenges, and produced a product that has the potential to revolutionize the market.

Part V
Appendix

24 Datasheets

The datasheets of the components used in this project is included in the following link of the GitHub project.

Link: https://github.com/avishkaherath/RFID-Access-Control-System

25 References

https://how2electronics.com/how-to-program-raw-esp8266-12e-f-chip-using-arduino-ide/
https://circuitjournal.com/esp8266-with-arduino-ide
https://diyables.io/products/door-sensor
https://diyi0t.com/active-passive-buzzer-arduino-esp8266-esp32/
https://arduino-esp8266.readthedocs.io/en/latest/boards.html
https://randomnerdtutorials.com/esp8266-pinout-reference-gpios/