

Bank Locker Security System Report

Executive Summary

This report presents the development and implementation of a secure bank locker system utilizing RFID and GSM technologies, controlled by an ESP32 microcontroller. The system is designed to ensure that only authorized users can access the locker, with unauthorized access triggering an SMS alert to a registered mobile number. The project aims to enhance security through reliable user authentication and real-time alerting mechanisms.

1. Introduction

The Bank Locker Security System is a critical application designed to safeguard valuable assets stored in lockers. Traditional security methods often fall short in providing robust protection against unauthorized access. This project leverages modern technologies—RFID for user identification and GSM for real-time alerting—to create a secure and reliable locker access system.

2. System Design

Flowchart

The system operates through a structured sequence of steps:

1. **User Scans RFID Tag:** The user places an RFID tag near the reader.
2. **ESP32 Verifies Tag ID:** The microcontroller reads and verifies the tag ID.
3. **Valid Access:** If the tag ID matches the authorized list, the locker opens via a servo motor.

4. **Invalid Access:** If the tag ID is unauthorized, an SMS alert is sent via the GSM module, and a buzzer is activated.
5. **Logging Access Attempts:** All access attempts are logged for security monitoring.

The system components are interconnected as follows:

- **RFID Module:** Reads the RFID tag and sends the data to the ESP32.
- **ESP32 Microcontroller:** Processes the RFID data and controls the servo motor and GSM module.
- **Servo Motor:** Opens and closes the locker based on ESP32 commands.
- **GSM Module:** Sends SMS alerts for unauthorized access.
- **Buzzer:** Alerts for unauthorized access attempts.
- **LCD Display:** Shows authentication status.
- **Power Supply:** Provides power to the system.

3. Components and Specifications

Key Components

- **ESP32 Microcontroller:** Central processing unit with Wi-Fi and Bluetooth capabilities.
- **RFID Module (MFRC522):** Reads RFID tags for user identification.
- **RFID Tags (Passive Cards):** Used for user authentication.
- **GSM Module (SIM800L/SIM900):** Sends SMS alerts for unauthorized access.

- **Servo Motor:** Opens and closes the locker.
- **LCD Display (16x2) with I2C:** Displays authentication status.
- **Buzzer:** Alerts for unauthorized access.
- **Power Supply (5V Adapter):** Provides power to the system.

Specifications

- **RFID Frequency:** 13.56 MHz
- **GSM Frequency:** 900/1800 MHz
- **Servo Motor:** SG90, 180-degree rotation
- **LCD Display:** 16x2 characters, I2C interface
- **Buzzer:** Passive buzzer, 5V

4. System Operation

RFID Module

The RFID module reads the tag ID and sends it to the ESP32 for verification. The tag ID is a unique identifier for each user.

ESP32 Microcontroller

The ESP32 processes the RFID data and checks if the tag ID is authorized. Based on the verification result, it controls the servo motor and GSM module.

Servo Motor

The servo motor is controlled by the ESP32 to open and close the locker. It rotates to 90 degrees to unlock and returns to 0 degrees to lock.

GSM Module

The GSM module sends an SMS alert to a registered mobile number in case of unauthorized access. The message includes a notification of the attempted access.

Buzzer

The buzzer activates for a short duration to alert of unauthorized access attempts.

LCD Display

The LCD display shows the authentication status, indicating whether access is granted or denied.

5. Implementation

Arduino Code

The following Arduino code implements the core functionality of the bank locker security system:

```
cppCopy
```

```
#include <WiFi.h>
```

```
#include <SPI.h>
```

```
#include <MFRC522.h>
```

```
#include <Servo.h>
```

```
#include <TinyGsmClient.h>
```

```
#define SS_PIN 5
```

```
#define RST_PIN 27
```

```
#define SERVO_PIN 18
```

```
#define BUZZER_PIN 19
```

```
#define RXD2 16
```

```
#define TXD2 17
```

```
Servo lockerServo;
```

```
HardwareSerial sim800(1);
```

```
MFRC522 mfrc522(SS_PIN, RST_PIN);
```

```
String authorizedUID = "12345678"; // Replace with your actual RFID tag UID
```

```
void setup() {
```

```
    Serial.begin(115200);
```

```
    sim800.begin(115200, SERIAL_8N1, RXD2, TXD2);
```

```
    SPI.begin();
```

```
    mfrc522.PCD_Init();
```

```
    lockerServo.attach(SERVO_PIN);
```

```
    pinMode(BUZZER_PIN, OUTPUT);
```

```
    Serial.println("Bank Locker System Initialized (ESP32)");
```

```
}
```

```
void loop() {
```

```
if (!mfrc522.PICC_IsNewCardPresent() ||  
!mfrc522.PICC_ReadCardSerial())
```

```
    return;
```

```
    String uid = "";
```

```
    for (byte i = 0; i < mfrc522.uid.size; i++)
```

```
        uid += String(mfrc522.uid.uidByte[i], HEX);
```

```
    Serial.println("Scanned UID: " + uid);
```

```
    if (uid == authorizedUID) {
```

```
        Serial.println("Access Granted");
```

```
        lockerServo.write(90);
```

```
        delay(5000);
```

```
        lockerServo.write(0);
```

```
    } else {
```

```
        Serial.println("Access Denied - Sending Alert");
```

```
        digitalWrite(BUZZER_PIN, HIGH);
```

```
        sim800.print("AT+CMGF=1\r");
```

```
        delay(1000);
```

```
        sim800.print("AT+CMGS=\"+919876543210\"\r"); // Change to  
your mobile number
```

```
        delay(1000);
```

```
    sim800.print("Unauthorized Access Attempted!");  
    sim800.write(26);  
    digitalWrite(BUZZER_PIN, LOW);  
}  
delay(2000);  
}
```

6. Future Enhancements

Biometric Authentication

Integrating a fingerprint scanner will add an additional layer of security by requiring biometric verification.

Face Recognition

Adding an ESP32-CAM module for face recognition will further enhance security by verifying the user's identity through facial recognition.

Cloud-Based Access Logs

Storing access logs in the cloud will enable remote monitoring and analysis of access attempts, providing valuable insights for security improvements.

AI for Anomaly Detection

Implementing AI algorithms to detect and flag unusual access patterns will enhance the system's ability to identify potential security threats.

7. Conclusion

The Bank Locker Security System using RFID and GSM technologies provides a robust solution for secure locker access. The integration of modern technologies ensures high security and reliability. Future enhancements, such as biometric authentication and cloud-based logging, will further strengthen the system's capabilities. This project demonstrates the potential of combining RFID, GSM, and microcontroller technologies to create secure and efficient access control systems.