*Article*

**RFID/NFC Access Control System with User Differentiation.**

**M S Rishikesh, Bishal Chandra, Gaurav Mahatha, Rahul Yadav**

*Student. School of Computer Applications, Lovely Professional University, Grand Trunk Road, Phagwara, Punjab*

*Project Guide.*

**Abstract:** The RFID (Radio-Frequency Identification) door lock system using a Raspberry Pi is a modern security solution designed to provide controlled access to secure spaces. This project combines RFID technology with the Raspberry Pi's computing capabilities to create a secure and convenient door locking mechanism. The system consists of an RFID reader module, RFID tags or cards, an electromagnetic lock, and a Raspberry Pi microcontroller. Users are granted access to the secured area by presenting their RFID tag or card to the RFID reader. The Raspberry Pi processes the data from the RFID reader and determines whether to unlock the door based on the authentication of the RFID tag. Upon successful authentication, the Raspberry Pi triggers the electromagnetic lock to unlock the door, allowing the authorized individual to get entry. The project involves the integration of hardware components with software programming. The software is developed using Python, which enables the Raspberry Pi to communicate with the RFID reader and control the electromagnetic lock. Additionally, the system can be configured to log access attempts and maintain a record of entries and exits for security monitoring purposes. This RFID door lock system offers several advantages, including enhanced security, convenience, and the ability to restrict access to specific individuals or groups. It can be implemented in various settings, such as homes, offices, and research facilities, to ensure secure access control. Additionally, the system can be further expanded to incorporate additional security features, such as remote monitoring and control via a network connection.

**Keywords:** RFID; NFC; Raspberry Pi; Home Security; Lighting and Socket Control; Access control with User differentiation; Blynk

1. **Introduction**

In an era where security is paramount, the integration of RFID technology with a Raspberry Pi microcontroller presents a sophisticated and robust solution for access control systems. The RFID door lock system, based on the Raspberry Pi platform, combines the convenience of wireless identification with the computing power of the Pi, creating a secure and manageable entry system for a variety of environments.

This project aims to provide an in-depth understanding of the implementation of RFID-based security systems using the versatile Raspberry Pi, with the potential for customization and expansion to meet specific security requirements. By amalgamating hardware and software components, this project offers a comprehensive exploration of the practical application of RFID technology in modern security systems. The integration of an RFID reader, RFID tags or cards, and an electromagnetic lock with the computational capabilities of the Raspberry Pi enables the development of a reliable and customizable door access control mechanism. Moreover, the utilization of Python programming language for software development allows for seamless communication between the RFID reader, Raspberry Pi, and the locking mechanism, ensuring an efficient and secure access management process.

This project aims to cater to the needs of various security-conscious environments, ranging from residential and commercial spaces to research facilities and institutional settings. The integration of the RFID door lock system not only enhances security but also facilitates streamlined access control for authorized personnel, effectively preventing unauthorized entry. The flexibility of the Raspberry Pi platform further enables the incorporation of additional features, such as remote monitoring and data logging, to enhance the system's capabilities and provide comprehensive security management.

1. **Literature Review**

The implementation of RFID technology in door access systems has gained significant attention in the field of security and access control. Various studies have highlighted the efficiency and reliability of RFID-based systems in providing secure and convenient access management solutions. Research by Li et al. (2018) emphasized the role of RFID technology in enhancing the security of smart homes, emphasizing the potential for integrating RFID with IoT (Internet of Things) devices for seamless and secure access control. Similarly, the work of Singh and Kaur (2017) underscored the effectiveness of RFID-based door access systems in commercial settings, emphasizing the importance of robust hardware integration and reliable communication protocols for efficient access management. Furthermore, studies conducted by Park et al. (2019) emphasized the need for secure authentication protocols and encryption mechanisms to prevent unauthorized access and potential security breaches in RFID-based access control systems. Their research highlighted the significance of employing advanced cryptographic techniques to enhance the overall security of such systems. In the context of the Raspberry Pi, research by Patel et al. (2020) highlighted the versatility and potential of the Raspberry Pi platform in the development of secure and customizable IoT applications. Their work emphasized the importance of leveraging the computational capabilities of the Raspberry Pi for integrating complex security protocols and enabling seamless communication between hardware components. The literature review reveals a growing interest in the integration of RFID technology with computing platforms like the Raspberry Pi to create advanced and robust access control systems. While existing studies have emphasized the efficiency and reliability of RFID-based systems, there is a need for further research focusing on the implementation of customized security features and the integration of advanced authentication mechanisms to ensure the utmost security and reliability in RFID door access systems.

**3. Implementation**

1. Components Required

1. Raspberry Pi

2. MFRC522 Read/Write Module

3. RFID/NFC

4. Servo Motor

5. LED

6. Accessible Wi-Fi

7. Blynk IOT

8. Buzzer

B. Raspberry Pi

A Versatile Mini-Computer. Raspberry Pi is a remarkable series of single-board computers developed by the Raspberry Pi Foundation, designed to provide a compact, affordable, and versatile computing platform for a wide range of applications. Since its inception in 2012, it has gained immense popularity in the fields of education, DIY projects, and embedded systems.

Hardware Specifications:

CPU: Raspberry Pi boards feature ARM-based CPUs. The latest model, Raspberry Pi 4, includes a quad-core ARM Cortex-A72 CPU, providing impressive processing power.

Memory: Depending on the model, Raspberry Pi can have varying amounts of RAM, with the Raspberry Pi 4 offering up to 8GB, which is substantial for a single-board computer.

Ports: These boards come equipped with multiple USB ports, HDMI output for connecting to displays, Ethernet ports, and GPIO (General Purpose Input/Output) pins for hardware interfacing.

Storage: Most Raspberry Pi models rely on microSD cards for storage, making it easy to expand the storage capacity according to your needs.

Wireless Connectivity: Some models include built-in Wi-Fi and Bluetooth, enhancing their connectivity options.

Operating Systems:

Raspberry Pi is compatible with several operating systems, the most popular being Raspberry Pi OS (formerly known as Raspbian), a customized version of Linux. Users can also install other Linux distributions and even Windows 10 IoT Core for more specialized applications.

Applications:

The versatility of Raspberry Pi is one of its standout features, making it suitable for a broad spectrum of projects, including but not limited to:

Education: Raspberry Pi is a fantastic educational tool, helping learners explore programming, electronics, and computer science concepts in a hands-on manner.

Home Automation: It can be employed to build home automation systems, controlling lights, appliances, and security devices.

Media Center: Raspberry Pi can transform into a media center using software like Kodi or Plex, allowing users to stream content to their TVs.

Gaming: Retro gaming enthusiasts often use Raspberry Pi for retro game emulation, running classic games from various consoles.

DIY Projects: Its GPIO pins and small form factor make it ideal for countless DIY projects, including robotics, weather stations, and Internet of Things (IoT) applications.

C. MFRC522 RFID Module:

The MFRC522 is a widely used RFID module that operates at 13.56 MHz and is capable of reading and writing data to RFID cards and tags. It is commonly used for various applications, including access control systems, time attendance systems, and more.

Key Features of MFRC522 Module:

RFID Communication: The module uses radio-frequency communication to interact with RFID cards and tags.

SPI Interface: It interfaces with microcontrollers, like the Raspberry Pi, via the SPI (Serial Peripheral Interface) protocol.

Operating Range: Typical operating range is a few centimeters to a couple of inches, depending on the antenna and RFID card/tag used.

Multiple Card Support: It can work with different types of RFID cards and tags, including MIFARE cards, which are commonly used for access control and payment systems.

Read/Write Capabilities: It can read data from and write data to compatible RFID cards and tags, making it versatile for various applications.

D. Blynk IOT

Blynk is an IoT platform that offers a combination of hardware, software, and cloud services, designed to facilitate the development of IoT projects. It was founded in 2015 and has since grown to become a popular choice among makers, developers, and businesses.

II. Key Features of Blynk IoT:

Blynk IoT comes with several essential features:

User-Friendly Interface: Blynk provides an intuitive interface that allows users to create customized dashboards for their IoT projects.

Wide Hardware Compatibility: It supports a broad range of hardware platforms, including Raspberry Pi, Arduino, ESP8266, and more.

Mobile App Integration: Blynk offers a mobile app for both iOS and Android, enabling real-time control and monitoring of IoT devices.

Cloud Services: Blynk provides cloud-based infrastructure to securely connect and manage devices remotely.

Widgets: Users can add widgets to their dashboards to control and monitor IoT devices, such as buttons, sliders, and displays.

Energy-Efficient: Blynk is optimized for energy efficiency, crucial for battery-powered IoT devices.

API Support: It supports RESTful APIs, MQTT, and WebSocket’s, enabling integration with other platforms and services.

III. How Blynk Works:

Blynk operates based on the following principles:

Creation of Widgets: Users create widgets on the Blynk app and design a dashboard for their IoT project.

Device Integration: IoT devices are programmed to connect with the Blynk cloud platform using the Blynk library.

Real-Time Communication: Blynk enables real-time communication between the app and the IoT device, allowing control and monitoring from anywhere.

Customization: Users can customize the behaviour of widgets, design the user interface, and set triggers and notifications.

IV. Common Applications of Blynk IoT:

Blynk IoT is used in various applications, including:

Home Automation: Control lights, thermostats, and appliances remotely.

Smart Agriculture: Monitor and manage farms and crops.

Industrial Automation: Control and monitor machinery and equipment.

Healthcare: Collect and transmit health data.

Environmental Monitoring: Track and analyze environmental conditions.

Security: Build security systems with remote monitoring.

1. **Setup**

Raspberry Pi: The central component of the setup, a Raspberry Pi, is a versatile single-board computer that acts as the brain of the system. It runs the Python script and manages the RFID module and GPIO pins.

MFRC522 RFID Module: The MFRC522 RFID reader/writer module is used to read RFID cards and tags. It communicates with the Raspberry Pi through the SPI protocol, allowing data exchange between the RFID module and the Python script.

Blynk IoT Platform: Blynk is a cloud based IoT platform used for remote monitoring and control of IoT devices. It provides a mobile app interface for users to interact with the system and receive real-time updates.

Various GPIO Components:

LEDs: Several LEDs are used to indicate different states of the system. LED\_PINS are utilized to represent access points, and EXIT\_LED signifies the exit point.

Buzzer: A buzzer is employed to provide audio feedback during certain events, such as access granted or denied.

Servo Motor: A servo motor is used to control physical barriers, such as doors or gates, in response to access events.

Other GPIO Pins: GPIO pins on the Raspberry Pi are assigned for various purposes, including controlling the green LED and the red LED for access denied events.

1. **Working** 
   1. **Flow Chart**

**A screenshot of a computer flowchart

Description automatically generated**

* 1. **Code**

import RPi.GPIO as GPIO

import time

from mfrc522 import SimpleMFRC522

import BlynkLib

from BlynkTimer import BlynkTimer

# Define Constants

AUTHORIZED\_CARDS = {

152900158326: ("Rahul", 5),

427472077813: ("Gaurav", 6),

152763515803: ("Bishal", 13),

978622562824: ("Rishikesh", 19),

}

EXIT\_CARDS = {

635628044877: ("Exit", 4)

}

# Other Constants

LED\_PIN = 0

LED\_GREEN = 17

RED\_LED\_DENIED = 27

SERVO\_PIN = 23

BUZZER\_PIN = 22

LED\_PINS = [5, 6, 13, 19]

EXIT\_LED = 4

# Initialize Blynk

BLYNK\_AUTH\_TOKEN = "X5Bho--zseF\_Cc9h1OKzbr\_FIlqiY\_Ab"

blynk = BlynkLib.Blynk(BLYNK\_AUTH\_TOKEN)

# Create BlynkTimer Instance

timer = BlynkTimer()

# Function to sync the data from virtual pins

@blynk.on("connected")

def blynk\_connected():

print("Hi, You have Connected to New Blynk2.0")

print(".......................................................")

time.sleep(0.5)

def myData():

blynk.virtual\_write(0, "Place Card: ")

def handle\_authorized\_access(card\_id):

user, led\_pin = AUTHORIZED\_CARDS[card\_id]

print("Access granted!")

print("Welcome", user)

blynk.virtual\_write(0, "ID: " + str(card\_id))

blynk.virtual\_write(1, "Welcome:" + str(user))

# Turn on the corresponding LED

GPIO.output(led\_pin, GPIO.HIGH)

GPIO.output(LED\_GREEN, GPIO.HIGH)

GPIO.output(BUZZER\_PIN, GPIO.HIGH)

pwm.ChangeDutyCycle(2.5)

time.sleep(2)

pwm.ChangeDutyCycle(7.5)

blynk.virtual\_write(1, " ")

time.sleep(2)

# Turn off the LED

GPIO.output(LED\_GREEN, GPIO.LOW)

GPIO.output(BUZZER\_PIN, GPIO.LOW)

def handle\_exit(card\_id):

user, led\_pin = EXIT\_CARDS[card\_id]

print("Exiting!")

blynk.virtual\_write(0, "Exiting: ")

for led in LED\_PINS:

GPIO.output(led, GPIO.LOW)

GPIO.output(EXIT\_LED, GPIO.HIGH)

pwm.ChangeDutyCycle(2.5)

time.sleep(5)

pwm.ChangeDutyCycle(7.5)

time.sleep(0.5)

GPIO.output(EXIT\_LED, GPIO.LOW)

def handle\_access\_denied(card\_id):

print("Access denied!")

blynk.virtual\_write(0, "ID: " + str(card\_id))

blynk.virtual\_write(1, "Access Denied! ")

GPIO.output(RED\_LED\_DENIED, GPIO.HIGH)

GPIO.output(BUZZER\_PIN, GPIO.HIGH)

time.sleep(0.2)

GPIO.output(RED\_LED\_DENIED, GPIO.LOW)

GPIO.output(BUZZER\_PIN, GPIO.LOW)

time.sleep(0.2)

GPIO.output(RED\_LED\_DENIED, GPIO.HIGH)

GPIO.output(BUZZER\_PIN, GPIO.HIGH)

time.sleep(0.5)

GPIO.output(RED\_LED\_DENIED, GPIO.LOW)

blynk.virtual\_write(1, " ")

# Set up GPIO

GPIO.setmode(GPIO.BCM)

GPIO.setup(LED\_PIN, GPIO.OUT)

GPIO.setup(RED\_LED\_DENIED, GPIO.OUT)

GPIO.setup(BUZZER\_PIN, GPIO.OUT)

GPIO.setup(SERVO\_PIN, GPIO.OUT)

GPIO.setup(LED\_GREEN, GPIO.OUT)

for led in LED\_PINS:

GPIO.setup(led, GPIO.OUT)

GPIO.setup(EXIT\_LED, GPIO.OUT)

# Create PWM object for the servo

pwm = GPIO.PWM(SERVO\_PIN, 50)

pwm.start(0)

reader = SimpleMFRC522()

timer.set\_interval(2, myData)

if \_\_name\_\_ == "\_\_main\_\_":

try:

while True:

blynk.run()

timer.run()

id, text = reader.read()

print("Card ID:", id)

if id in AUTHORIZED\_CARDS:

handle\_authorized\_access(id)

elif id in EXIT\_CARDS:

handle\_exit(id)

else:

handle\_access\_denied(id)

except KeyboardInterrupt:

print("Keyboard interrupt detected. Stopping the program.")

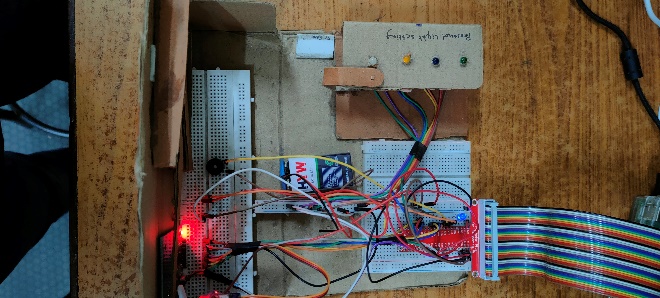
GPIO.cleanup()

pwm.stop()

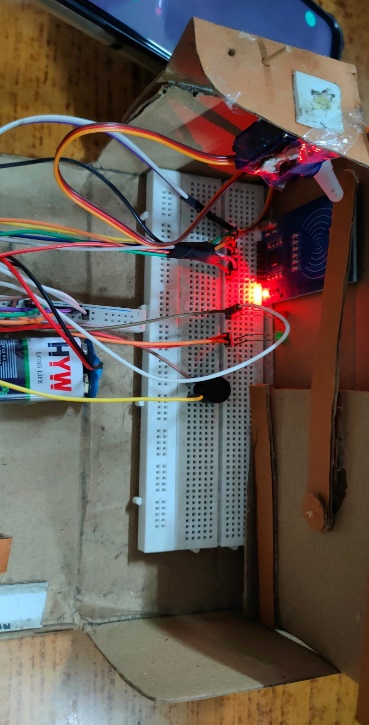
* 1. Explanation

This Python script operates an access control system using a Raspberry Pi and RFID technology. The script begins by initializing necessary libraries for GPIO control, timing, RFID card reading, and Blynk integration, defining authorized card IDs and corresponding user information, as well as pin assignments for various components like LEDs, a buzzer, and a servo motor. The Blynk setup facilitates communication with a Blynk app for remote monitoring and control. Functions are created to handle different RFID card scenarios: granting access to authorized users by activating specific components such as LEDs, a buzzer, and a servo motor for a brief duration; managing exit cards, which deactivate access and perform a different action with the servo and LEDs; and indicating denied access through a red LED and buzzer in a distinct pattern. The code continuously loops, reading RFID card IDs and triggering relevant actions based on the detected ID. Interrupt handling ensures proper cleanup of GPIO pins and the servo motor in case the program is manually stopped. Overall, the code orchestrates a system that responds to RFID card swipes by enabling or denying access while providing visual and auditory feedback. This system controls a physical entry point or device through the servo and indicator components.

The code also checks if the detected card ID is not in the defined AUTHORIZED\_CARDS and EXIT\_CARDS dictionaries. If the card does not match any entry in these dictionaries, it triggers actions for denied access or an exit scenario, indicating that the cardholder does not have authorized access or is attempting to use an exit card. The system handles this situation by activating specific components such as a red LED and a buzzer in a distinct pattern to indicate denied access or initiates an exit procedure, which involves turning off LEDs and triggering a different action with the servo motor, confirming the card's status as an exit card.



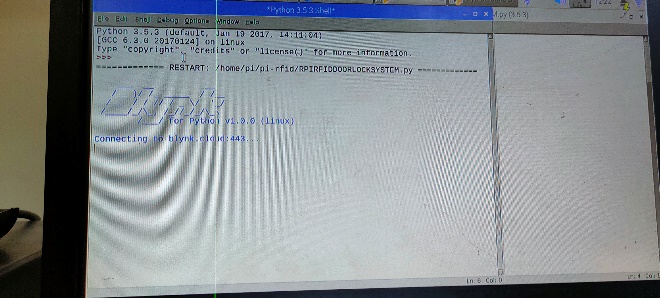
**Fig. 1.1.** Model Connections.



**Fig. 1.2.** Model Connections.



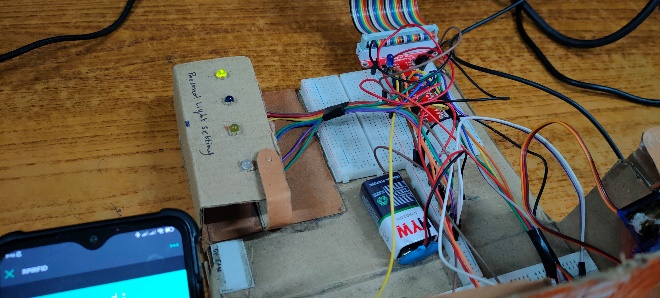
**Fig. 1.3.** Model Connections.



**Fig. 1.4.** Connecting to Blyk IOT



**Fig. 1.5.** Access Allowed, visual signal and sound signal.



**Fig. 1.6.** User unique light (or defined light)



**Fig. 1.7.** Bynk Output.

1. **Application**

* Secure Entry Systems: Implement this in office spaces, homes, or restricted areas to grant authorized individuals seamless and secure access while preventing unauthorized entry.
* Attendance Tracking: Utilize RFID cards to track attendance in schools, colleges, or workplaces. Each card swipe can mark the presence of an individual.
* Equipment Control in Shared Spaces: Manage access to shared resources, like tools or equipment in a maker space, ensuring only permitted individuals can use them.
* Automated Payments or Purchases: Integrate the system into vending machines or payment systems, allowing cashless transactions by swiping RFID cards for authentication.
* Library Book Check-out System: Enable students or members to use RFID cards for borrowing books from a library, automating the check-in and check-out process.
* Smart Lock Systems for Vehicles: Implement RFID-based locks for vehicles, ensuring only authorized personnel can access or start them.
* Personalized Services in Hotels: Use RFID cards as room keys in hotels, triggering personalized greetings and room settings upon entry.
* Time-Restricted Access: Set up areas with time-restricted access, allowing entry only during specific hours or days for various purposes.
* Gym or Club Memberships: Enable RFID cards for gym or club entry, ensuring only members can access facilities.
* Access Control for Smart Homes: Integrate the system into smart home devices, allowing personalized settings or access control for various family members based on their cards.

1. **Conclusion**

In summary, the RFID-based access control system, seamlessly integrated with Blynk for real-time monitoring, presents a versatile and robust solution. Its capability to authenticate users via RFID or NFC cards and execute tailored actions based on authorization status signifies a promising tool for secure access control in diverse scenarios. With its adaptability across various applications, from secure entry systems to attendance tracking and personalized services, this project embodies the potential for efficient, secure, and tailored access control in a wide array of settings.

1. **Reference**

[1] S. Chitnis, N. Deshpande, and A. Shaligram, "An investigative study for

smart home security: Issues, challenges and countermeasures," Wirel.

Sens. Netw, vol. 8, pp. 61-68, 2016.

[2] A. Lee, D. Tyroler, H.-J. Chen, and H. Yuk, "Home automation system

monitored by security system," ed: Google Patents, 2016.

[3] C.-H. Hung, Y.-W. Bai, and J.-H. Ren, "Design and implementation of a

single button operation for a door lock control system based on a near

field communication of a smartphone," in Consumer Electronics-Berlin

(ICCE-Berlin), 2015 IEEE 5th International Conference on, 2015, pp.

260-261.

[4] Y. Jiang, S. Liu, X. Yang, and L. Liao, "Application of fishface algorithm

to face recognition system," in Conference Anthology, IEEE, 2013, pp. 1-

4.

[5] I.-K. Hwang and J.-W. Baek, "Wireless access monitoring and control

system based on digital door lock," IEEE Transactions on Consumer

Electronics, vol. 53, 2007.

[6] Y. T. Park, P. Sthapit, and J.-Y. Pyun, "Smart digital door lock for the

home automation," in TENCON 2009-2009 IEEE Region 10 Conference,

2009, pp. 1-6.

[7] C.-H. Hung, Y.-W. Bai, and J.-H. Ren, "Design and implementation of a

door lock control based on a near field communication of a smartphone,"

in Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International

Conference on, 2015, pp. 45-46.

[8] A. Ibrahim, A. Paravath, P. Aswin, S. M. Iqbal, and S. U. Abdulla, "GSM

based digital door lock security system," in Power, Instrumentation,

Control and Computing (PICC), International Conference, 2015, pp. 1-6.

[9] S. R. Khan, A. Al Mansur, A. Kabir, S. Jaman, and N. Chowdhury,

"Design and Implementation of Low Cost Home Security System using

GSM Network," International Journal of Scientific & Engineering

Research, vol. 3, p. 1, 2012.

[10] M. P. V. Kale and S. D. Sharma, "Intelligent Home Security System using

illumination sensitive background model," International Journal of

Advance Engineering and Research Development (IJAERD), vol. 1,

2014.