Smart Door Lock Using Node MCU

Chandrasekhar Paseddula
Assistant Professor, ECE, GNITS, Hyderabad, India

Abstract: The Smart Door Lock System aims to offer convenience, security, and user-friendliness for homeowners. It lets them control their door from a distance. Users can register their device and operate the door using a mobile app or a web interface. After registration, they can open or close the door with a simple tap on their device. This eliminates the need for traditional door mechanisms or physical keys.

The system uses modern wireless technology to connect the smart doorbell and the door locking mechanism. Besides allowing remote control of the door, the system includes security features like video streaming, two-way communication with visitors, and motion sensors for safe access. This new approach to home automation gives users the ability to manage entry and exit points easily, improving home security and convenience.

IndexTerms - Smart Door lock System, Node MCU

I.INTRODUCTION

In today's security-focused world, traditional door locks often do not provide enough protection against unauthorized access. As security threats change, there is a greater need for reliable solutions that go beyond standard locking systems. This project aims to develop a smart door lock system with a high-resolution camera to improve security measures.

Fig 1.1 Smart Door Lock

In Fig 1.1, the smart door lock uses facial recognition technology to verify users and allow entry only for authorized individuals. This removes the risks of lost keys or stolen access codes. The system also has remote access, enabling homeowners to monitor and control entry to their property from anywhere using a smartphone or computer. This feature offers convenience, allowing users to provide temporary access to visitors or service personnel without being there in person..

By combining artificial intelligence, secure cloud storage, and real-time alerts, this smart lock provides an effective way to improve home security. If there are any unauthorized attempts, the system can capture images, send instant notifications, and record access data for future reference. This gives homeowners complete visibility and control over who enters their property.

This smart door lock system combines advanced technology with an easy-to-use design. It marks an important improvement in home security solutions. Homeowners can enjoy greater peace of mind and better protection.

1.1 Literature Survey

Misal et al. (2014) created a door locking and unlocking system that uses SMS technology with GSM/GPRS services. This system lets users control and secure their doors from a distance. It offered convenience and improved security by connecting mobile communication with home automation [1].

Murru et al. (2020) suggested a similar idea. They proposed using a fingerprint sensor to unlock doors. This improves home automation by removing the need for traditional keys. It also boosts security with biometric authentication [2].

Sharma et al. (2023) examined how deep learning could help regulate subscription-based services to support SDG Goal 12, which focuses on sustainable consumption and production. Their findings suggested that AI could play an important role in promoting responsible consumption, especially in the post-COVID era, when economic models needed to adjust to new consumption patterns [3].

Siddiquee et al. (2022) created an IoT-based agricultural monitoring system. Their system used algorithms to track environmental conditions in real-time. This helped farmers optimize their operations and improve crop yields [4].

Belmon and Auxillia (2022) introduced a system for continuous glucose monitoring that uses IoT technology for diabetic patients. This system provides real-time data collection, which helps improve the management of chronic diseases [5].

Bouazzi et al. (2022) looked into the future of healthcare monitoring in smart cities. They proposed using LoRaWAN-based WBAN technology to offer low-power, wide-area connectivity for tracking patient health. This supports the concept of smart healthcare systems [6].

The study by Ahmed et al. (2022) looked at a recommender system that used devices and text reviews. Their system provided personalized recommendations by using real-time data, which improved user experiences in different areas. Meanwhile, in the field of medical diagnostics [7].

Gunjan et al. (2022) used grey wolf optimization and recurrent neural networks to find lung cancer from CT scans. Their combined method focused on delivering an early diagnosis that could improve the detection and treatment of lung cancer [8].

Gaddam et al. (2022) studied how deep learning can detect facial emotions. This is an important area in human-computer interaction. The system could be useful in several fields, such as surveillance, customer service, and improving user experience [9].
Mani et al. (2022) made important contributions by combining potential shape signatures with neural networks for medical image classification. Their work focused on improving the accuracy of medical diagnoses, especially for complex diseases [10].
Pathak and Gupta (2020) gave an overview of natural computing methods, including neural networks and genetic algorithms. They highlighted how these methods can be used to tackle complex, real-world problems [11].
Kotha and Pavan (2022) provided a survey on deep learning techniques for object detection. They compared models like YOLO, SSD, and R-CNN regarding performance, efficiency, and real-time use [12].
Security and authentication were improved by Gunjan et al. (2020). They used machine learning for biometric authentication, focusing on extracting and classifying biometric features to ensure secure identity verification. This is related to educational technology [13].
Singh et al. (2022) compared their adaptive tutoring system, SEIS Tutor, with existing platforms. They showed that personalized and adaptive learning can significantly improve student outcomes and engagement [14].
In medical applications, Mokhlesabadifarahani and Gunjan (2015) studied EMG signal characteristics using fuzzy networks. Their work helped improve understanding of muscle contractions and supported the design of biomedical devices for rehabilitation purposes [15].
Usman et al. (2021) proposed a threshold detection method for optical fiber communication. This method, based on parametric distribution fitting, aimed to improve the reliability and efficiency of communication channels [16].

Kumar et al. (2022) used a support vector machine (SVM) model to detect credit card fraud. Their system showed high accuracy in finding fraudulent transactions. This provides a safe solution for financial institutions [17].
In medical imaging, Prabhu Das and colleagues (2022) examined segmentation algorithms for contrast and non-contrast MRI images. Their research improved the accuracy of region-of-interest detection, which helps in medical diagnoses and imaging analysis [18].

1.2 Problem Statement

Conventional door locks can be easily bypassed, which increases the risk of break-ins and theft. Homeowners often struggle to verify who is at their door before granting access. This raises safety concerns. Current smart locks may offer remote control features but often do not have strong verification methods. This project aims to tackle these problems by creating a smart door lock system that combines a camera with facial recognition technology. This will provide secure and convenient access control while improving overall home security.

1.3 Aim of the Project

To design and implement a Smart Door Lock System using Node MCU, this system will have security features for efficient and secure access control.
It aims to use facial recognition technology to authenticate users, ensuring that only authorized people can enter. Additionally, it will allow remote access, enabling homeowners to monitor and control door access through a mobile app or web interface.
The integration of a camera module will improve security by capturing real-time images or videos of individuals requesting access.

II. METHODOLOGY

2.1 Existing Methods

1. Biometric Authentication

Biometric authentication in smart locks uses unique physical traits like fingerprints, facial recognition, or retina scans to allow access. This technology improves security because biometric data is very hard to copy. Unlike regular keys or PIN codes, you can't easily lose or share your fingerprints, which lowers the risk of unauthorized access. Many smart locks can store multiple fingerprints, so family members or trusted people can get in. Some advanced models use artificial intelligence to get better at recognizing fingerprints over time. However, harsh weather or dirty sensors can sometimes hurt the performance of fingerprint or facial recognition[10].

2. Remote Access

Remote access lets users control and monitor their smart locks from anywhere using a smartphone app. With Wi-Fi or Bluetooth, users can lock and unlock doors without being there in person. This feature is helpful for letting in guests, service providers, or delivery personnel without needing a physical key. Users can also check the lock's status in real-time, providing peace of mind even when they are away from home. Many smart locks allow temporary or scheduled access codes that expire automatically after a set time. However, for Wi-Fi-enabled locks, a stable internet connection is necessary for smooth operation [9].

3. Keyless Entry

Keyless entry removes the need for traditional metal keys. It uses PIN codes, smartphone apps, NFC, or biometrics to unlock doors. This change reduces the risk of losing keys and stops unauthorized key duplication. Some smart locks let users set different PIN codes for family members or guests, making it easier to manage access. Many models also include an auto-lock feature that secures the door after a set amount of time. This ensures safety even if someone forgets to lock it manually. In emergencies, some locks offer backup access methods, like a hidden keyhole or an external battery connection. While these locks are convenient, it's important to select a model with encryption and security features to protect against hacking attempts [1].

4. Alerts and Notifications

Smart locks with alert features send real-time notifications to the owner's phone about lock and unlock activities. These alerts can include details like the time of access and which user entered the home, aiding in security monitoring. Some locks also provide tamper alerts, letting users know if someone tries to break in or force the lock. Low battery warnings help prevent unexpected malfunctions, allowing for timely battery replacements. These notifications improve security by keeping users updated on all access-related activities. However, a strong Wi-Fi or Bluetooth connection is necessary to receive alerts without interruptions [19].

5. Integration with Smart Home Systems

Many smart locks can connect with home automation systems. This allows for easy control using smart assistants like Amazon Alexa, Google Assistant, or Apple HomeKit. Users can give voice commands to lock or unlock the door. They can also automate actions, such as turning on lights when the door is unlocked. Smart locks can work with security systems, sending alerts to home monitoring services if they detect suspicious activity. Users can set up routines, like locking the door automatically at night or when they leave home. This feature makes things more convenient and improves security, especially when paired with other smart home devices. However, it's important to ensure strong encryption and regular software updates to avoid security issues15].

2.2 Disadvantages of Existing Smart Door Lock Systems

High Initial Cost

Smart locks are significantly more expensive than traditional locks, making them less accessible for budget-conscious users.

Additional costs may include installation, smart home integration, or subscription fees for advanced security features.

Dependence on Power and Internet

Many smart locks rely on batteries or electricity, and a dead battery can result in a locked-out situation.

Wi-Fi or Bluetooth-based locks may become non-functional if there is a network outage or poor connectivity.

Vulnerability to Hacking and Security Risks

Some smart locks can be hacked through weak encryption, outdated firmware, or Bluetooth/Wi-Fi vulnerabilities.

If the associated app or cloud service is compromised, unauthorized access to the lock may become a risk.

Malfunctions and Sensor Issues

Biometric sensors (fingerprint, facial recognition) can sometimes fail due to dirt, moisture, or extreme weather conditions.

Technical malfunctions or software bugs may cause the lock to become unresponsive, requiring a manual override.

5. Limited Backup Options

Some keyless smart locks do not have a physical key backup, which can be problematic if the electronic system fails.

Temporary solutions like external battery ports or manual overrides may not always be reliable in emergencies.

2.3 Proposed Method

To deal with the high initial cost of smart door locks, users can choose budget-friendly models that focus on key features like PIN access and remote control. They should avoid pricey extras like cameras or fingerprint sensors. Installing the lock themselves can save on installation fees, and selecting brands that don't require monthly subscriptions helps prevent ongoing costs. Gradually adding to a smart home setup, instead of upgrading everything at once, can spread out expenses. Also, taking advantage of seasonal discounts or bundles can lower the total price. Finally, considering the long-term benefits such as better security, convenience, and possible increases in property value can justify the investment.

Smart locks usually depend on batteries or a steady power source. If the battery dies or there's a power failure, users might get locked out or lose some features. Most models give low-battery warnings, but ignoring them can cause problems. Also, smart locks that use Wi-Fi or Bluetooth can fail during internet outages or in places with weak signals. This limits remote access or control through apps. This reliance on power and network stability can be a drawback compared to traditional mechanical locks, which work without any outside energy.

Smart locks, like any connected device, are vulnerable to digital threats. If a lock has weak encryption, outdated firmware, or insecure Bluetooth or Wi-Fi connections, it can attract hackers. Cybercriminals may take advantage of these weaknesses to intercept data, gain unauthorized access, or control the lock from a distance. Furthermore, if the mobile app or cloud service connected to the lock is hacked, it could reveal user credentials or access logs, creating a serious security risk. This highlights the importance of regular software updates, strong encryption, and secure authentication in keeping a smart lock system safe.

Smart locks with biometric sensors, like fingerprint or facial recognition, can fail due to dirt, moisture, or extreme weather affecting sensor accuracy. These problems may stop authorized users from getting access, particularly in outdoor or busy areas. Also, technical issues or software bugs can make the lock freeze, lag, or stop responding entirely. In these situations, users may have to use a physical key or a manual override to get back in. This shows how important it is to pick a lock with solid backup options and to keep firmware updated regularly.

Certain keyless smart locks are made without a physical keyhole. They depend entirely on electronic access methods like PIN codes, biometrics, or mobile apps. While this gives a sleek and modern look, it can be a serious problem if the system fails because of dead batteries, software errors, or connectivity issues. Some models offer temporary solutions like external battery ports or emergency power contacts, but these may not work well in urgent situations or bad weather. The absence of a dependable manual override raises the risk of being locked out. Therefore, it is important to select smart locks with strong backup access options.

2.4 Advantages of Proposed Method:

1.Remote Control and Keyless Entry:

NodeMCU lets users lock and unlock the door from a smartphone app. This removes the need for physical keys.

2.Enhanced Security:

Smart locks provide features such as access logs, temporary access codes for guests or service providers, and integration with security systems. These features improve overall security.

3.Integration with Smart Home Systems:

NodeMCU-based smart locks can easily fit into current smart home systems. This lets users control several devices from one platform.

4.Convenience and Accessibility:

Smart locks provide more convenience and make it easier for people with mobility challenges or those who often forget their keys.

5.Cost-Effectiveness:

NodeMCU is a low-cost microcontroller, making it a budget-friendly choice for creating a smart door lock system.

6.Scalability and Flexibility:

The IoT-based design of NodeMCU makes it easy to scale and adjust. Users can add features or expand the system later on.

7.Real-time Monitoring:

The system can provide real-time monitoring of the door lock status. Users can check if the door is locked or unlocked from anywhere.

8.Activity Logs:

Smart locks can track access history. They give useful information about who entered or left the building and when.

III. HARDWARE COMPONENTS

The Components are used in the Smart Door Lock:

1. Node MCU(ESP8266)
2. ESP32-CAM
3. Relay Module
4. PIR Sensor
5. Lock
6. Buzzer
7. Connection Patch
8. Bluetooth
9. Cables

3.1 Node MCU (ESP8266)

In Fig 3.1 (a), the Node MCU ESP8266 development board includes the ESP-12E module, which has the ESP8266 chip featuring a Tensilica Xtensa 32-bit LX106 RISC microprocessor. This microprocessor supports RTOS and runs at an adjustable clock frequency of 80 MHz to 160 MHz. The Node MCU comes with 128 KB of RAM and 4 MB of Flash memory for storing data and programs. Its strong processing power, built-in Wi-Fi and Bluetooth, and Deep Sleep Operating features make it suitable for IoT projects.

Node MCU can be powered using a Micro USB jack and VIN pin (External Supply Pin). It supports UART, SPI, and I2C interface. We can easily observe in the Fig 3.1 (b)

Fig 3.1 (a) Node MCU(ESP8266)

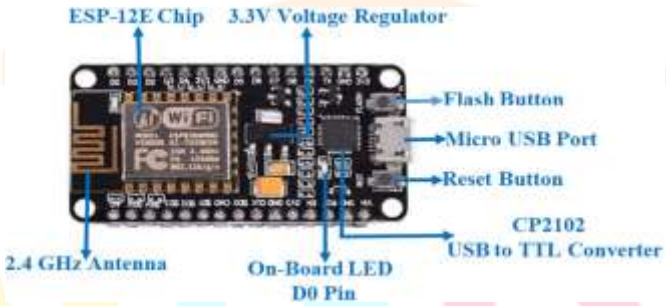

Fig 3.1 (b) Node MCU(ESP8266) pinout

Node MCU ESP8266 Specifications & Features

The module features a Tensilica 32-bit RISC CPU Xtensa LX106 running at 80 MHz, with 3.3V operating voltage and 7–12V input range. It provides 16 digital I/O pins, 1 analog input, and supports UART, SPI, and I²C interfaces. Equipped with 4 MB flash, 64 KB SRAM, and an onboard CP2102 USB-TTL converter for plug-and-play use, it also includes a PCB antenna. Compact and efficient, the module is ideal for IoT and embedded applications requiring reliable wireless communication.

Advantages:

1. Wi-Fi Connectivity

The ESP8266 comes with built-in Wi-Fi, which makes it very easy to connect to the internet or local networks without needing additional hardware like a Wi-Fi shield or dongle the Fig 3.1 (a) shown in the above.

2. Low Cost

NodeMCU boards are fairly cheap. They have Wi-Fi capabilities and can run complex code. This makes them a great choice for projects that need to stick to a budget.

3. Compact and Lightweight

The NodeMCU is small and lightweight. This makes it a good fit for compact designs. It can be easily added to small projects without using much space.

4. Easy Programming (Arduino IDE Compatible)

NodeMCU works with the Arduino IDE. This lets developers write and upload code in a familiar environment. As a result, it's easy for beginners and accessible for those who know Arduino development.

5. Wide Support and Documentation

The ESP8266 and NodeMCU have a large, active online community. There are many tutorials, forums, and open-source libraries available to help solve any problems that come up during development.

6. Low Power Consumption

The ESP8266 mainly focuses on Wi-Fi connectivity. However, it can also operate in low-power modes. This feature makes it a good choice for battery-powered projects and applications where saving energy matters.

3.2 ESP32-CAM

The ESP32-CAM is a small, low-power camera module based on the ESP32, as shown in Fig(a) 3.2. It features an OV2640 camera and includes an onboard TF card slot. This board has 4MB of PSRAM, which buffers images from the camera for video streaming and other tasks. This allows for higher quality pictures without crashing the ESP32. Additionally, it has an onboard LED for flash and several GPIOs to connect peripherals. You can also see the pin diagram in Fig(b) 3.2.

.

Fig 3.2 (a) ESP32-CAM Module

Fig 3.2 (b) ESP32-CAM Pinout

Features:

The ESP32-CAM is a compact IoT module based on the ESP32-D0WD processor, integrating Wi-Fi, Bluetooth 4.2, and an OV2640 camera with flash. It supports TF cards up to 4 GB for image storage and offers multiple low-power modes, with deep sleep current as low as 6 mA. Supporting JPEG, BMP, and Grayscale formats, it provides UART, SPI, I²C, and PWM interfaces through a 9-pin header. Operating at 5 V, the module includes 32 Mbit flash, 512 KB RAM, and 4 MB PSRAM, with transmit power up to 17 dBm and sensitivity to –90 dBm. Compact (40.5 × 27 × 4.5 mm) and efficient, the ESP32-CAM is ideal for smart surveillance, wireless monitoring, intelligent agriculture, QR code scanning, and facial recognition applications.

3.3 Relay Module

A relay module is a switching device, the control circuit that operates with low-power signals. In the Fig 3.3 tells that it enables a low-power supply circuit to switch on or regulate a high-power supply circuit without integrating it with the same circuit or electrical appliance. In other words, relay modules are employed to break the different parts of the given system to mitigate the problems of electrical coupling or failure.

Fig 3.3 Relay Module

3.4 PIR Sensor(passive Infrared Sensor)

A PIR sensor (Passive Infrared Sensor) is a type of sensor that detects motion by measuring infrared radiation emitted by objects in its field of view, typically focusing on body heat from humans or animals as shown in the Fig 3.4.

Fig 3.4 PIR Sensor

How It Works:
Infrared Radiation: All objects, including humans, emit infrared radiation (heat) in the form of infrared light. PIR sensors detect this radiation.
Sensor Elements: A PIR sensor typically consists of a pair of pyroelectric sensors (or a single one), which are sensitive to infrared radiation. These sensors detect any changes in the levels of infrared radiation within their detection range.
Detection: When an object (like a human body) moves within the sensor's range, it causes a change in the infrared radiation that the sensor detects. If the radiation levels increase or decrease due to the movement of a warm object (like a person), the sensor registers this change and triggers an output signal (e.g., turning on a light or activating an alarm).
Detection Field: PIR sensors have a detection range that usually spans from a few meters to tens of meters. They also have a broad detection field, typically between 90° and 180°. These sensors perform best when positioned in spots where they can sense movement, like hallways, doorways, or rooms.
Applications:
Security Systems: PIR sensors are often used in motion-detection security alarms or systems.
Lighting Automation: PIR sensors can work in smart lighting systems that turn lights on or off when someone enters or leaves a room.
Home Automation: They are used to control devices or systems based on whether a person is present.
Energy Management: In commercial buildings, PIR sensors help save energy by managing lighting according to room occupancy.
Advantages:
Security Systems. PIR sensors are commonly used in motion-detection security alarms or systems.
Lighting Automation. PIR sensors can be used in smart lighting systems that turn lights on or off when someone enters or leaves a room.
Home Automation. These sensors control devices or systems based on human presence.
Energy Management. In commercial buildings, PIR sensors help save energy by controlling lighting based on room occupancy.

3.5 Lock
The door locks provide essential safety and security to one's home. They are pretty necessary to keep your place, be it home or work, safe and ensure privacy. With the technological developments and needs for functionality, we have different types of door locks to match the requirements of other individuals. For instance, a home's central door
place may require a tight security lock, compared to a private door or an office chamber or gates.
Different types of Locks:
Padlocks:

Fig 3.5 (a) Padlock
A padlock is a portable locking mechanism typically used to secure doors, gates, lockers, or other objects to prevent unauthorized access.
A Padlocks is shown in the Fig 3.5 (a) consist of a body, a shackle (the U-shaped metal part), and a mechanism that locks and unlocks the shackle. They can be opened with a key, a combination, or even electronically in some modern designs.
Lever Handle:

Fig 3.5 (b) Lever Lock
In the Fig 3.5 (b) Lever Lock tells that the Lever handles are a popular choice to use for the inside doors within homes or offices. They are popular mainly in commercial settings and shops or offices. There is a sizeable pushdown-style handle in this kind of lock that works to open the lock so open the lock
Rim or Mortise Lock:

Fig 3.5 (c) Rim or Mortise Lock
Rim or mortise door lock types are the most popular choice for large commercial doors, glass doors, or fancy buildings. In this case, rim cylinder locks are attached and mounted inside the door, which looks like a long metal piece extended outside. A box lock is often set within this rim and mortise towards the edge. The Fig 3.5 (c) is shown in the above.

Barrel Bolt:

Fig 3.5 (d) Barrel Bolt

The barrel bolts are a kind of sliding bolts that fall under the traditional category. Yet, they are among the safest to use for secure living inside. It is shown in the Fig 3.5 (d). In these old door lock types, a barrel sliding bolt helps lock and unlock, and the two components that go are fixed on the door frame and the door.

IV. WORKING PRINCIPLE OF SMART DOOR LOCK BY USING NODEMCU

4.1 Working Principle:

The system is powered by a 12V DC supply, regulated by the RPS. When the PIR sensor detects motion, it sends a signal to the Node MCU. The ESP CAM can capture images, possibly triggered by motion detection or at regular intervals, sending the data to the Node MCU. The Node MCU processes the data from the sensors. Based on the programmed logic, the Node MCU can activate the relay module to control the lock (open/close) and/or trigger the buzzer to sound an alarm. The system may also be connected to a network via Wi-Fi (integrated into the Node MCU), allowing for remote monitoring and control.

Power-Up and Initialization:

Once the system is powered on, the NodeMCU (ESP8266) initializes and starts controlling the system. It will check the state of the PIR sensor to detect any movement near the door.

The ESP32-CAM is powered on and ready to capture video or images.

Motion Detection (PIR Sensor):

The PIR sensor constantly monitors for motion. When it detects movement (for example, someone approaching the door), it sends a signal to the NodeMCU to trigger the next step.

The NodeMCU can then instruct the ESP32-CAM to capture an image or stream video.

Verification via ESP32-CAM (Face Recognition/Video Feed):

The ESP32-CAM takes a picture or streams live video to a connected device (e.g., a smartphone or cloud server) for authentication. You can use facial recognition or other verification methods, like sending the image to a mobile app or server, to check if the person at the door is authorized. In this situation, the ESP32-CAM could either upload the image to a server for remote verification or use a local model for facial recognition.

Relay Control for Locking/Unlocking:

Based on the verification results:

If the person is verified (authorized), the NodeMCU sends a signal to the Relay Module to unlock the door.

If the person is not verified (unauthorized), the NodeMCU can trigger the buzzer to sound an alert.

The Relay Module acts as a switch that controls the lock mechanism. When the relay is activated, the lock will be opened; when it's deactivated, the door remains locked.

Feedback (Buzzer):

The Buzzer can be used to provide audio feedback:

If the motion is detected, but no authorization occurs, the buzzer can sound, indicating an error or intruder.

If the person is authorized and the door unlocks, a short positive sound can be triggered as confirmation.

User Interaction (Optional Features):

For enhanced functionality, you could include an app or web interface to remotely check the video feed from the ESP32-CAM and unlock the door.

The app could send a command to the NodeMCU to trigger the relay to unlock the door remotely.

System Reset (Optional):

After a successful unlock or lock operation, the system could automatically reset to check for further movement or verify new users.

4.2 Block Diagram

The block diagram of the prepared system is shown in the fig 4.1

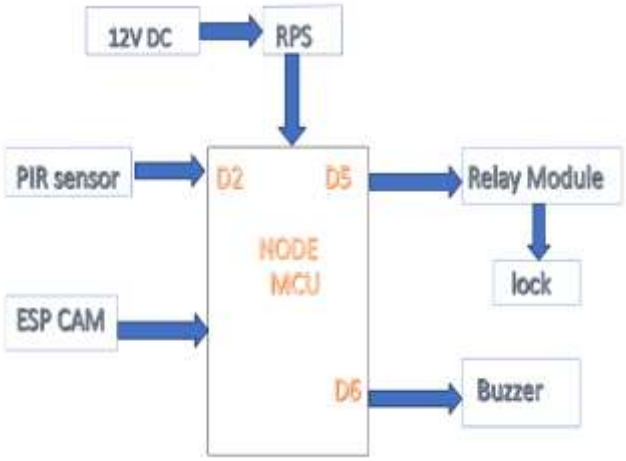

Fig 4.1 Block Diagram of Smart Door Lock

This smart door system combines several parts to improve security and automation. At its center is the NodeMCU (ESP8266), which handles all logic operations, Wi-Fi connections, and communication between devices. A PIR sensor picks up motion near the entrance, which triggers the system to start authentication. The ESP32-CAM takes images or video, allowing for facial recognition to verify users. Once authentication is successful, the NodeMCU activates a relay module that controls the electronic lock, granting access. A buzzer gives audio feedback to indicate success, failure, or alerts. The whole system runs on a regulated power supply (RPS), providing stable and enough energy for all parts to work reliably. This setup offers secure, automated smart door access.

4.3 Flow chat

The Flow Chat of the Smart Door Lock is shown in the Figure 4.2

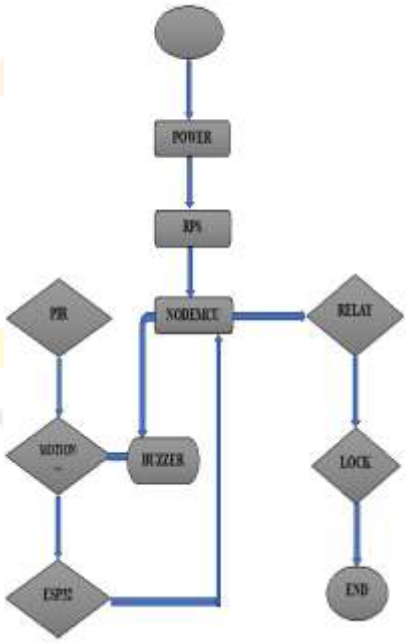

Fig 4.2 Flow chat of smart Door Lock

The smart door lock system begins with a START point, followed by powering on the device. The system then initializes the ESP32 or NodeMCU microcontroller, which acts as the brain of the setup.

After initialization, the system continuously monitors the environment using a PIR (Passive Infrared) motion sensor. This sensor detects any motion near the door. If no motion is detected, the system keeps looping and monitoring

If motion is detected, the system proceeds to trigger a buzzer to alert the user or intruder of detection. Next, the system initiates an RPS verification, where the user must provide valid credentials either via a keypad, remote control, mobile app, or biometric scan. If the RPS input is invalid, the system may sound an alert and return to monitoring. If the RPS input is valid, the system activates a relay module which in turn unlocks the electronic lock on the door.

After the door is unlocked, the system either waits for a timeout period or a manual lock command, after which it will lock the door again, completing the process. The system finally reaches the END of the flow.

V. RESULTS AND DISCUSSION

5.1 Result:

The Smart Door Lock system improves security and convenience by providing a keyless and controlled access method. The final implementation works well with authentication methods such as passwords, RFID, biometrics, or mobile-based access. Overall, the Smart Door Lock is shown in Fig 5.1.

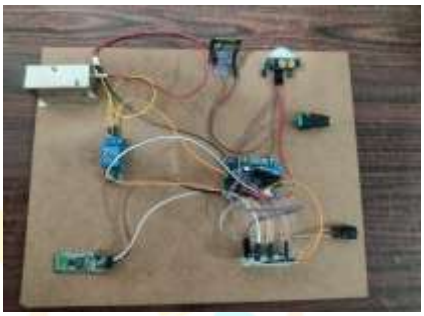

Fig 5.1 Smart Door Lock

5.2 Applications:

1. Home Automation

Remote Locking and Unlocking: The Node MCU allows control of door locks from a distance through a mobile app, web interface, or voice commands using Alexa or Google Assistant. Homeowners can lock or unlock their doors from anywhere in the world.

Integration with Home Automation Systems: It can work with home automation platforms like Open HAB, Home Assistant, or others. This provides centralized control of various devices, including locks.

2. Security Systems

Time-based Access Control: The system can be set up to allow access only during specific hours of the day or night. This is helpful for workplaces or rental properties.

Biometric Authentication: Connecting the Node MCU with biometric systems, like fingerprint scanners or RFID cards, can improve security by making sure only authorized people can unlock the door.

Alerts and Notifications: The system can send alerts to the owner through email, SMS, or mobile apps when the door is unlocked or tampered with, raising awareness about possible intrusions.

3. Smart Lock with RFID or Keypad Access

RFID or Keypad-based Entry: Node MCU can control a smart door lock that allows users to access the door with RFID tags, NFC-enabled devices, or PIN codes entered on a keypad. Multiple User Support: The system can store RFID tags or PIN codes for multiple users, making it easy to manage access. This feature is helpful in settings like offices or shared spaces.

4. Integration with Other IoT Devices

Security Camera Integration: The system can connect to a security camera to record video when someone interacts with the door. This video can be saved either locally or remotely.

Smart Lights and Alarms: Unlocking the door could trigger other actions, such as turning on lights, activating alarms, or automatically opening gates and garages as part of a larger IoT setup.

.

5. Automated Check-in for Rental Properties (Airbnb/Hotels)

Remote Access for Guests: For rental properties, the system lets hosts send unique codes or keys to guests. This makes check-in and check-out easy. It removes the need for physical keys and enables secure, remote access management.

Time-limited Access: The Node MCU-based smart lock can be programmed to give guests temporary access, such as during their stay, and will automatically expire after that time.

6. Voice Control (AI Integration)

Voice Assistants: Using AI assistants like Amazon Alexa or Google Assistant lets users unlock the door with voice commands. This is especially helpful for people with mobility challenges or those who need to unlock doors without using their hands.

Hands-free Operation: Users can command the system to lock or unlock doors without having to physically touch the door.

7. Visitor Management System

Scheduled Access for Visitors: Homeowners can set specific times for visitors to enter, making it easier to manage deliveries or visits from family members when they are not home.

Temporary Access: The system can create temporary access codes or keys for visitors, which will expire after a set time.

8. IoT-based Monitoring

Access Log Management: Node MCU can keep a record of who unlocked the door, when it happened, and from which device. This helps maintain a history of door access that can be checked at any time.

Battery Monitoring: The system can also track the battery level of the lock to make sure it stays functional. It sends alerts when the battery is getting low.

9. Integration with Smart Home Ecosystem

Smart Home Central Hub: Node MCU can fit into a bigger smart home system. It can connect with other smart devices like thermostats, security cameras, and lighting systems. For example, unlocking the door could prompt the thermostat to change the temperature for comfort.

10. Emergency Unlocking

Override Mechanism: In an emergency, such as a fire, medical issue, or power failure, the system can be set up to unlock right away or allow for manual override to keep people safe.
Battery Backup: Node MCU-based systems can have a battery backup that keeps the lock working even when the power goes out. This way, users can still unlock the door.
5.3 Advantages:
Keyless Entry: Eliminates the need to carry or duplicate physical keys.
Improved Security: Offers strong authentication methods like passwords or biometrics.
Remote Access (if applicable): Allows unlocking using a mobile app or access card.
Access Logs: Records entry and exit times for security tracking.
Customizable Permissions: Grants temporary or role-based access for different users.
Disadvantages:
Power Dependency: Requires battery or electrical power, which can fail without proper maintenance.
Risk of Hacking: If not secured well, the system could be open to unauthorized access.
Higher Initial Cost: More expensive than traditional locks because of technology integration.
Technical Failures: Hardware or software problems may lead to lockouts.
Connectivity Issues (if applicable): Wi-Fi or Bluetooth locks may not work well if the network is unstable.

VI. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion:

The Smart Door Lock system offers a secure and efficient option compared to traditional locks. It includes features like password protection, biometric authentication, and remote access control. These features improve both safety and convenience for homes, offices, and commercial spaces. While there are some challenges, such as reliance on power and possible cybersecurity risks, good security practices and regular upkeep can increase reliability. This project shows a modern way to handle access control and security solutions.

6.2 Future Scope:

The Smart Door Lock system can be improved with these advancements:
IoT & Cloud Integration: This would allow real-time alerts and remote access from anywhere.
Enhanced Encryption: Stronger security protocols can prevent unauthorized access.
Multi-Lock Synchronization: This connects several smart locks in a building for centralized control.
Energy Efficiency Improvements: Developing low-power locks with better battery backup or using alternative power sources like solar energy.
Voice & Gesture Control: Hands-free unlocking through voice commands or motion sensors.
Integration with Emergency Systems: Automatic unlocking during fire alarms or emergencies would allow for quick evacuation.

REFERENCES

P. Misal, M. Karule, D. Birdawade, A. Deshmukh, and M. Pathak, “Door locking/unlocking system using SMS technology with GSM/GPRS services,” International Journal of Electrical Communication and Computer Engineering, vol. 5, no. 4, pp. 192–294, 2014.

Y. Sharma, R. Sijariya, and P. Gupta, “How deep learning can help in regulating the subscription economy to ensure sustainable consumption and production patterns (12th Goal of SDGs),” in Deep Learning Technologies for the Sustainable Development Goals, Springer Nature, Singapore, 2023, pp. 1–20.

K. N. E. A. Siddiquee et al., “Development of algorithms for an IoT-based smart agriculture monitoring system,” Wireless Communications and Mobile Computing, vol. 2022, pp. 1–16, 2022.

M. R. Mani, T. Srikanth, and C. Satyanarayana, “An integrated approach for medical image classification using potential shape signature and neural network,” in Machine Learning and Internet of Things for Societal Issues, Springer Nature, Singapore, 2022, pp. 109–115.

I. Bouazzi et al., “Future trends for healthcare monitoring system in smart cities using LoRaWAN-based WBAN,” Mobile Information Systems, 2022.

R. Pathak and S. S. Gupta, “A study on natural computing: a review,” in Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications (ICDSMLA 2019), Springer, Singapore, 2020, pp. 1975–1983.

N. Singh, V. K. Gunjan, and M. M. Nasralla, “A parametrized comparative analysis of performance between proposed adaptive and personalized tutoring system ‘seis tutor’ with existing online tutoring system,” IEEE Access, vol. 10, pp. 39376–39386, 2022.

D. K. R. Gaddam et al., “Human facial emotion detection using deep learning,” in Proceedings of the 2nd International Conference on Data Science, Machine Learning and Applications (ICDSMLA 2020), Springer, Singapore, 2022, pp. 1417–1427.

[A. P. Belmon and J. Auxillia, “IoT-based continuous glucose monitoring system for diabetic patients using sensor technology,” in Machine Learning and Internet of Things for Societal Issues, Springer Nature, Singapore, 2022, pp. 35–41.

[B. Mokhlesabadifarahani and V. K. Gunjan, “EMG signals characterization in three states of contraction by fuzzy network and feature extraction,” Springer, 2015.

M. K. Kotha and K. K. Pavan, “Deep learning for object detection: a survey,” in Proceedings of the International Conference on Computer Vision, High Performance Computing, Smart Devices and Networks (CHSN-2020), Springer Nature, Singapore, 2022, pp. 61–84.

V. K. Gunjan, N. Singh, F. Shaik, and S. Roy, “Detection of lung cancer in CT scans using grey wolf optimization algorithm and recurrent neural network,” Health Technology, vol. 12, no. 6, pp. 1197–1210, 2022.

R. Pathak, B. Soni, and N. B. Muppalaneni, “Role of blockchain in health care: a comprehensive study,” in Proceedings of 3rd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, Springer, Singapore, vol. 540, 2023.

S. Prabhu Das, B. N. Jagadesh, and B. Prabhakara Rao, “Performance evaluation of segmentation algorithms in non-contrast and contrast MRI images for region of interest,” in Proceedings of the International Conference on Computer Vision, High Performance Computing, Smart Devices and Networks (CHSN-2020), Springer Nature, Singapore, 2022, pp. 95–111.

M. Ahmed et al., “Rating-based recommender system based on textual reviews using IoT smart devices,” Mobile Information Systems, 2022.

V. K. Gunjan, P. S. Prasad, R. Pathak, and A. Kumar, “Machine learning methods for extraction and classification for biometric authentication,” in Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications (ICDSMLA 2019), Springer, Singapore, 2020, pp. 1984–1988.

M. Usman et al., “Threshold detection scheme based on parametric distribution fitting for optical fiber channels,” Recent Advances in Computer Science and Communications, vol. 14, no. 2, pp. 409–415, 2021.

S. Kumar, V. K. Gunjan, M. D. Ansari, and R. Pathak, “Credit card fraud detection using support vector machine,” in Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications (ICMISC 2021), Springer, Singapore, 2022, pp. 27–37.