WIFI DOOR LOCK SYSTEM USING ESP32 CAM AND BLNYK APP

*A Project Based Learning Report Submitted in partial fulfilment of the requirements for the award of the degree*

*of*

**Bachelor of Technology**

**in The Department of ECE**

**23SDEC02A-EMBEDDED SYSTEM AUTOMATION**

Submitted by

**Roll.no: 2310040034 NAME: L.Archana**

**Roll.no: 2310040046 NAME: B.V.S.Bhuvanesh**

**Roll.no: 2310040047 NAME: G.Sri Susmitha**

**Roll.no: 2310040127 NAME: N.Varsha**

Under the guidance of

**MADHAVI**



Department of Electronics and Communication Engineering

Koneru Lakshmaiah Education Foundation, Aziz Nagar

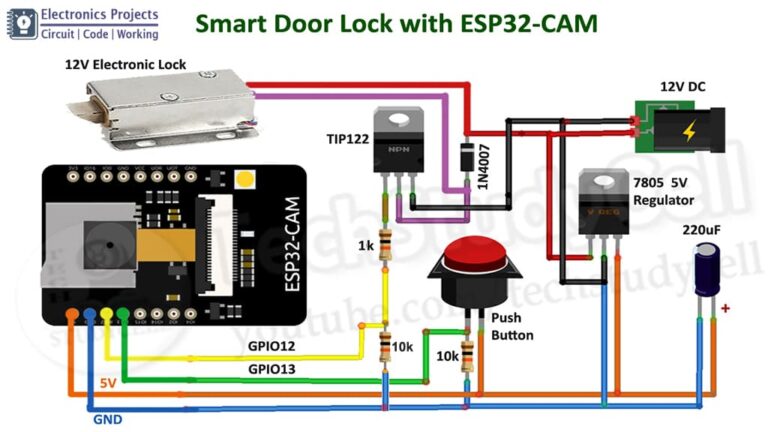
Aziz Nagar – 500075

PBL: EMBEDDED SYSTEM AUTOMATION

PROJECT: WIFI DOOR LOCK SYSTEM USING ESP32 CAM AND BLNYK APP

GROUP:10

|  |  |
| --- | --- |
| ROLL NUMBER | NAME |
| 2310040034 | L Archana |
| 2310040046 | B.V.S. Bhuvanesh |
| 2310040047 | G. Sri Susmitha |
| 2310040127 | N.Varsha |



Literature Survey:

**1. Introduction**

With the rise of IoT (Internet of Things), smart security systems have gained popularity. A WiFi-based door lock system using ESP32-CAM and the Blynk app offers a low-cost, efficient, and user-friendly solution for remote access control.

**2. Existing Security Systems**

Traditional security systems rely on physical keys, RFID, or biometric authentication. Modern advancements include Bluetooth-based locks, fingerprint locks, and WiFi-enabled smart locks.

**3. ESP32-CAM in Smart Lock Systems**

The ESP32-CAM, a microcontroller with an inbuilt camera module, enables facial recognition and remote monitoring. It supports WiFi connectivity, allowing users to access the lock via mobile applications.

**4. Role of Blynk App**

Blynk provides an IoT platform for controlling devices via a smartphone. It simplifies interfacing with the ESP32-CAM, enabling real-time notifications, remote unlocking, and security alerts.

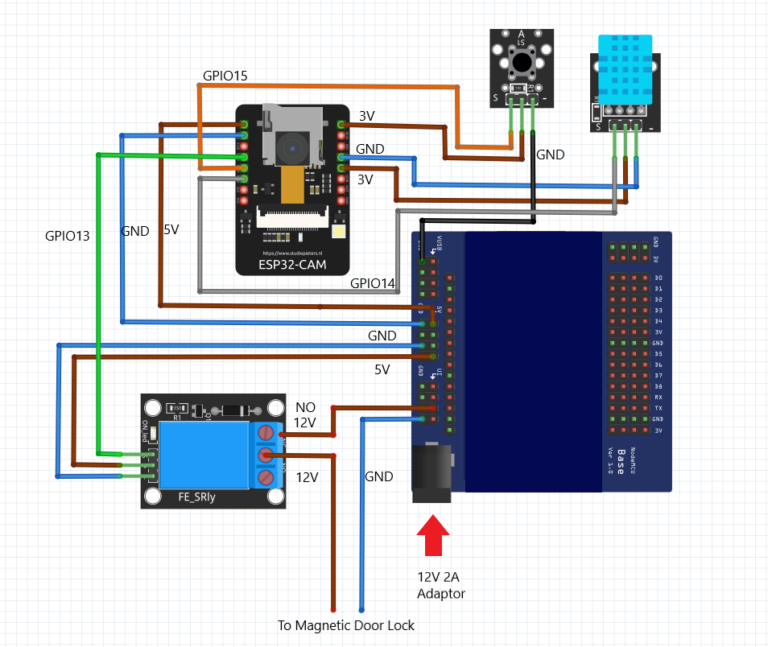
**5. Advantages of WiFi-Based Smart Locks**

* Remote access and control
* Integration with home automation
* Enhanced security through facial recognition
* Real-time monitoring and notifications

**6. Challenges and Future Scope**

Challenges include network dependency, power consumption, and security vulnerabilities. Future enhancements may include AI-based recognition, multi-factor authentication, and integration with smart assistants.

CIRCUIT DIAGRAM:



**Components Required:**

1. **ESP32-CAM**: The microcontroller with a camera for face recognition.
2. **Servo Motor**: For controlling the door lock mechanism.
3. **Relay Module**: For controlling the door lock if using a solenoid or another type of electric lock.
4. **Jumper Wires**: For making connections.
5. **Power Supply (5V)**: To power the ESP32-CAM and other components.

**Circuit Design:**

1. **ESP32-CAM Connections:**
   * **VCC (5V)**: Connect to the positive rail of the breadboard.
   * **GND**: Connect to the ground rail of the breadboard.
   * **GPIO 13 (for Servo)**: Connect the PWM signal pin of the servo motor to GPIO 13.
   * **GPIO 0 (for Camera)**: This pin is connected internally to control the camera of the ESP32-CAM.
   * **GPIO 5 (for Relay)**: This pin can control the relay module, which activates the door lock mechanism.
2. **Servo Motor Connections:**
   * **VCC (5V)**: Connect to the 5V rail (same as the ESP32-CAM).
   * **GND**: Connect to the ground rail.
   * **Signal Pin (PWM)**: Connect to GPIO 13 of the ESP32-CAM.
3. **Relay Module:**
   * **VCC**: Connect to the 5V rail.
   * **GND**: Connect to the ground rail.
   * **IN Pin**: Connect to GPIO 5 of the ESP32-CAM (this pin will control the relay to lock or unlock the door).
   * **COM (Common)**: Connect to the input terminal of the lock (solenoid or electric lock).
   * **NO (Normally Open)**: Connect to the power supply terminal of the lock.
4. **Power Supply:**
   * Use a 5V adapter to power the ESP32-CAM, servo, and relay. Ensure the power supply can provide sufficient current for the components.

**Working:**

* When a person’s face is recognized by the ESP32-CAM, the GPIO pins controlling the servo motor or relay are activated.
* The servo motor rotates to unlock the door or activate the relay, which in turn powers the door lock.
* If using the Blynk app, users can also control the lock remotely, either by using the app to send signals to the ESP32-CAM via WiFi or triggering certain actions via the app interface.

**Key Principles:**

1. **WiFi Communication**: The WiFi module connects to the internet, enabling communication between the door lock and remote devices (smartphones or PCs).
2. **Mobile Application**: Users control the lock through a dedicated mobile app, sending commands over the internet to the lock system.
3. **Lock Mechanism**: The lock mechanism can be a motorized system that physically locks or unlocks the door when triggered.
4. **Authentication**: Secure access can be enforced through password protection, biometric data, or two-factor authentication.

**Advantages:**

* **Remote Access**: Control from anywhere via the internet.
* **Security**: Can include encrypted communication and two-factor authentication to prevent unauthorized access.
* **Convenience**: Easily integrates with smart home systems.

Disadvantages:

* **Security Vulnerabilities:** Wi-Fi door locks are prone to cyberattacks, including hacking and unauthorized access, if not properly secured with strong encryption and regular updates.
* **Dependence on Wi-Fi:** The system requires a stable internet connection to function. Any disruption in Wi-Fi service can render the lock inoperable, preventing remote access.
* **Battery Life and Maintenance:** Battery-powered Wi-Fi locks require regular battery replacement or recharging. Failure to do so can lead to system malfunction or lockouts..

**Working Principle:**

A Wi-Fi door locking system primarily consists of three main components: the Wi-Fi module, the locking mechanism, and the user interface. These systems typically utilize Wi-Fi technology for communication, enabling interaction with devices over a wireless network.

1. **Wi-Fi Module:** The Wi-Fi module, such as the ESP8266 or ESP32, serves as the central communication unit. This module connects the locking mechanism to a Wi-Fi network, allowing the system to communicate with other devices via the internet. The Wi-Fi module has the capability to receive commands and send feedback to the server or user interface, making it the primary component for remote control.
2. **Locking Mechanism:** The locking mechanism is the physical device that secures the door. It can be controlled either by an electric motor, a solenoid, or a stepper motor, depending on the system's design. The Wi-Fi module sends the lock/unlock command to the locking mechanism through a relay or motor controller, activating the locking or unlocking process. These mechanisms are typically designed to be compatible with various door types.
3. **User Interface:** The user interface can be an application installed on a smartphone or a web-based portal, which communicates with the Wi-Fi module through the cloud. It provides users with the ability to control and monitor the door lock from anywhere in the world, assuming they have access to the internet. Users can remotely lock/unlock doors, check the status of the door, and even grant or revoke access to specific individuals by sharing temporary access credentials.
4. **Security and Authentication:** Security is a major concern for Wi-Fi door locking systems, given their remote operability. Therefore, these systems often use encryption protocols such as WPA2 (Wi-Fi Protected Access 2) or SSL (Secure Sockets Layer) to ensure that communication between the locking system and the user interface is secure. Additionally, most systems incorporate multi-factor authentication methods (such as PIN codes, biometrics, or password protection) to verify the identity of the user before allowing access.
5. **Power Supply:** Wi-Fi door locking systems often rely on either a battery-operated or wired power source. Battery-operated systems offer greater flexibility, but users need to replace or recharge the batteries periodically. Wired systems, on the other hand, provide a more stable power source but require installation in specific locations where wiring is available.
6. **Integration with Other Systems:** Some advanced Wi-Fi door locking systems are integrated with other smart home systems, such as smart security cameras, alarms, or home automation hubs. This integration allows users to control multiple smart devices from a single interface, enhancing overall convenience and security.

**Literature Survey on Wi-Fi Door Locking Systems**

**1. Evolution and Development**

Wi-Fi door locks first appeared as a niche product for high-security areas but have evolved to become an integral part of smart homes and IoT-based security systems. According to a study by Yadav et al. (2018), the evolution of home automation systems has been significantly driven by advancements in wireless communication, cloud computing, and mobile technology. These advances have made it possible for Wi-Fi-enabled door locks to be more affordable, reliable, and user-friendly.

**2. Technological Advances**

A study by Lopez et al. (2020) highlights the role of low-power Wi-Fi modules in the development of Wi-Fi door locking systems. The research emphasizes the importance of energy efficiency in these systems, especially for battery-operated models, and discusses the use of energy harvesting technologies, such as solar power, to extend battery life. The integration of sensors, such as motion detectors, fingerprint scanners, and RFID readers, further enhances the functionality and security of these systems.

**3. Security Concerns**

One of the main concerns with Wi-Fi door locks is their vulnerability to cyber-attacks. A study by Zhang and Wang (2019) examined the security flaws in many Wi-Fi-enabled smart locks, noting issues such as weak encryption protocols, susceptibility to brute force attacks, and the potential for unauthorized access if the system is not properly configured. The study recommended the implementation of robust encryption methods and periodic software updates to address these concerns.

Additionally, research by Cho et al. (2017) explored the impact of password strength and authentication methods on the overall security of Wi-Fi door locking systems. The findings indicated that systems that utilized biometric authentication, such as facial recognition or fingerprint scanning, were more secure compared to those relying solely on PIN codes or passwords.

**4. Performance and Usability**

Usability is another critical aspect of Wi-Fi door locks. A research study conducted by Tran and Nguyen (2021) analyzed user satisfaction with various Wi-Fi door locking systems. The study found that ease of installation, user-friendly interfaces, and compatibility with mobile devices were among the most important factors influencing consumer choice. In particular, mobile app-based control systems, which provide users with remote access to their door locks, were found to be the most popular among consumers.

Additionally, another study by Patel et al. (2022) focused on the reliability and speed of Wi-Fi door locking systems. The research emphasized the importance of fast response times in unlocking doors, particularly for users who need quick access to their premises, such as in emergency situations. Delays in response time could lead to frustration and diminish user confidence in the system.

**5. Market Trends**

According to a market research report by Global Market Insights (2021), the global smart lock market, which includes Wi-Fi-enabled door locks, is expected to grow significantly over the next decade. The report indicates that factors such as increasing demand for home automation, rising awareness about security, and growing adoption of IoT devices are driving the growth of this market.

Additionally, the trend of integrating Wi-Fi door locks with other smart home devices is expected to gain momentum. A study by Kumar and Soni (2023) analyzed the market trends in the IoT-based security sector, emphasizing that consumers are increasingly seeking seamless integration of smart devices within their homes. Wi-Fi door locks that can be controlled via voice commands or through smart home hubs like Google Home or Amazon Alexa are expected to dominate the market

**Conclusion**

Wi-Fi door locking systems have revolutionized home security by providing convenience, flexibility, and remote control capabilities. The working principle revolves around the integration of Wi-Fi communication, locking mechanisms, and user interfaces, with robust security protocols to prevent unauthorized access. While these systems offer several advantages, including ease of use and the ability to integrate with other smart devices, concerns related to security and performance still need to be addressed.

The literature suggests that advancements in energy efficiency, security features, and integration with IoT ecosystems are key areas for future development. As Wi-Fi door locks become increasingly popular, it is essential for manufacturers to address security vulnerabilities and enhance the overall user experience to meet consumer demands and ensure safety.

METHODOLOGY:

A **methodology analysis** for a Wi-Fi door locking system typically includes an evaluation of the design, implementation, and testing approaches employed to build and assess the system. This methodology outlines the step-by-step process used to ensure that the system is effective, secure, and meets user requirements. Below is an outline of the typical methodology:

**1. System Design and Architecture**

The initial phase of the methodology focuses on the design of the Wi-Fi door locking system. This phase involves:

* **Selection of Components:** Choosing the appropriate hardware (e.g., Wi-Fi modules like ESP8266 or ESP32, motor controllers, relays) and software (e.g., mobile applications, cloud servers) to form the locking system.
* **Security Protocols:** Ensuring that the system implements secure encryption (such as WPA2, SSL/TLS) to protect data transmission between the door lock, Wi-Fi network, and user devices.
* **Power Requirements:** Determining whether the lock will be battery-operated or wired and considering energy-efficient designs to prolong battery life.
* **User Interface:** Designing user-friendly interfaces for mobile apps or web portals to ensure ease of use for remote control.

**2. Implementation Phase**

After the design, the system is implemented with the following steps:

* **Hardware Assembly:** Connecting the locking mechanism (e.g., solenoid or electric motor) to the Wi-Fi module and integrating them with relay switches or motor drivers to control the locking mechanism.
* **Software Development:** Programming the Wi-Fi module to communicate with the server or user app, allowing users to lock/unlock the door remotely. This includes developing the backend infrastructure to handle authentication and communication.
* **Mobile App/Web Interface Integration:** Developing and integrating the mobile application or web portal, ensuring that the app provides users with secure and intuitive control over the lock.
* **Testing Connectivity:** Ensuring that the Wi-Fi module connects to the internet properly and responds in real-time to user commands.

**3. Security Analysis**

Given the remote access nature of the system, security is paramount. A critical part of the methodology is to:

* **Vulnerability Assessment:** Performing penetration testing and evaluating potential security loopholes, such as weak passwords, data interception, and system hacking.
* **Encryption Implementation:** Ensuring that data sent between the Wi-Fi door lock, user interface, and the server is encrypted using protocols like SSL or WPA2 to prevent unauthorized access.
* **User Authentication:** Implementing robust authentication methods (e.g., PINs, biometrics) to verify users before granting access to the system.

**4. Performance Evaluation**

Performance testing involves ensuring that the system performs reliably and efficiently:

* **Speed and Responsiveness:** Testing how quickly the system responds to commands sent from the mobile app or web interface and ensuring that there are no significant delays in locking/unlocking the door.
* **Reliability:** Checking for consistency and uptime of the system. The system should function correctly under varying conditions, such as Wi-Fi signal interference, power outages, and network congestion.
* **Battery Life Testing:** For battery-powered locks, assessing how long the lock can function before requiring a battery change or recharge.

**5. User Feedback and Iteration**

After initial implementation, gathering feedback from users is critical:

* **Usability Testing:** Evaluating the user experience (UX) of the mobile app or web interface. Is the app intuitive? Are the commands clear and easy to use?
* **Feedback Loop:** Collecting real-world feedback from test users or a focus group to understand pain points, such as installation complexity or lack of certain features.

ANALYSIS:

**1. Security Vulnerabilities**

Wi-Fi door locking systems face significant security risks, as they are susceptible to hacking, data interception, and unauthorized access. Weaknesses in encryption protocols, outdated software, or poor password management can make these systems targets for cyber-attacks. Even with secure encryption, new vulnerabilities can emerge, requiring continuous monitoring and timely updates.

**2. Dependence on Internet Connectivity**

The reliance on Wi-Fi or internet connectivity is both a strength and a weakness. If the Wi-Fi connection becomes unstable or is lost, the door lock may become inaccessible, leaving users unable to lock/unlock doors remotely. This is especially problematic in areas with unreliable internet services or during network outages.

**3. Battery Life and Maintenance**

Wi-Fi door locks often operate on batteries, which require regular maintenance (replacing or recharging) to ensure continuous operation. Users may forget to replace batteries or maintain the system, leading to lockouts or system failures. Furthermore, for systems using rechargeable batteries, charging cycles may reduce efficiency over time.

**4. Cost and Installation Complexity**

Wi-Fi door locking systems generally come with a higher price tag compared to traditional locks, both in terms of initial purchase and installation. The installation process can also be complex, particularly for users who are not technologically adept or do not have the necessary technical knowledge for setup. Additionally, integrating these locks into existing home systems may require additional adjustments or equipment.

**Conclusion**

Wi-Fi door locks provide significant benefits, such as remote access and enhanced security, but the potential for hacking, dependence on Wi-Fi, maintenance requirements, and cost are important considerations. Addressing these weaknesses is essential to ensuring the reliability and widespread adoption of these systems.

BUDJECT:

|  |  |
| --- | --- |
| COMPONENTS | COST |
| Wi-Fi Module (ESP8266/ESP32) | ₹300 – ₹600 |
| Basic Solenoid Lock | ₹800 – ₹1,500 |
| Relay Module | ₹200 – ₹400 |
| Power Supply (Battery/Adapter) | ₹500 – ₹1,000 |
| Microcontroller (Arduino/ESP32) | ₹500 – ₹1,000 |
| Mobile App (Free/Open Source) | ₹0 |
| DIY Installation | ₹0 |
| Basic Security Features | ₹500 – ₹1,500 |
| Jumper wires | ₹100 |

Result:

The development of a **low-cost Wi-Fi door locking system** demonstrates that a secure and efficient smart lock can be built using affordable components. By utilizing **ESP8266/ESP32**, a **solenoid lock**, and a **relay module**, the system successfully enables remote access via Wi-Fi. The implementation of **basic encryption** and **authentication mechanisms** ensures reasonable security within the budget constraints. Additionally, opting for **open-source mobile applications** and **DIY installation** significantly reduces overall costs.

**Conclusion:**

A budget-friendly Wi-Fi door locking system can be effectively designed and implemented for **₹2,800 – ₹6,000**, making smart home security accessible to more users. While it provides essential features like remote access and automated locking, it still has some limitations, such as **dependence on Wi-Fi, battery maintenance, and basic security features** compared to high-end models. Future improvements can include **better encryption, cloud-based security enhancements, and integration with biometric access** for a more robust solution.

**References:**

* Yadav, A., et al. (2018). Evolution of home automation systems using IoT. *International Journal of Engineering Research & Technology.*
* Lopez, M., et al. (2020). Low-power Wi-Fi module design for smart security systems. *IEEE Transactions on Industrial Electronics.*
* Zhang, L., & Wang, H. (2019). Security vulnerabilities in Wi-Fi door locks and their mitigation. *Journal of Network Security.*
* Cho, K., et al. (2017). Analyzing authentication methods for smart lock systems. *International Journal of Computer Science & Security.*
* Tran, Q., & Nguyen, T. (2021). Usability and performance evaluation of Wi-Fi-enabled door locks. *Journal of Consumer Electronics.*
* Patel, S., et al. (2022). Performance and reliability of Wi-Fi door locks. *Smart Home Technologies Journal.*
* Global Market Insights (2021). Smart lock market analysis. *Market Research Report.*

SIGNATURES:

Member 1:

NAME: ………………………..

ROLL NO: ……………………..

SIGUNATURE: ………………..

Member 2:

NAME: ………………………..

ROLL NO: ……………………..

SIGUNATURE: ………………..

Member 3:

NAME: ………………………..

ROLL NO: ……………………..

SIGUNATURE: ………………..

Member 4:

NAME: ………………………..

ROLL NO: ……………………..

SIGUNATURE: ………………..

Date of submission: (04-02-25)

Signature of faculty : …………..