RFID-Based Digital Door Locking System

Sudeep fullel and Dikshant Madai
BSc (Hons) Computer and Data Science
Sunway College Kathmandu
Kathmandu, Nepal

***Abstract* — The RFID-Based Digital Door Locking System is a product of modern computing, incorporating technologies like IoT, fog computing, edge computing, and cloud computing. It leverages cutting-edge concepts in computing to enhance its functionality and security. This system combines the power of an Arduino microcontroller with a servo motor, IR sensors, and RFID technology to provide a secure and efficient access control mechanism. Users can register RFID cards, and when a registered card is scanned, the system activates the servo motor, opening the door lock. In contrast, unregistered cards trigger a "wrong card" response displayed on an LCD. This paper delves into the background research on IoT and its current and future trends, emphasizing the pivotal role of 5G technology and blockchain. It discusses the essential hardware components, the mechanism, and security considerations of the RFID-Based Digital Door Locking System, offering recommendations for further enhancements and additional programming. The system showcases the convergence of technology to create a reliable, secure, and user-friendly access control solution.**

***Keywords*— IoT, RFID, Arduino, Servo Motor, Access Control, Security, 5G, Blockchain, Edge Computing, IoT Trends, Smart Devices, User Management.**

IoT, Fog computing, Edge computing, and Cloud computing are just a few of the cutting edge technologies that make up the fast evolving field of modern computing. (De Donno et al., 2019). Among these, Edge computing plays a critical role in modern computing as it enables computation near the network's edge, allowing for both downstream data from cloud services and upstream data from IoT services to be processed quickly and efficiently (Shi et al., 2016). Another important component of modern computing is Fog computing, which serves as a mediatory layer between Cloud computing and IoT and operates in a distributed manner (Mahmud et al., 2017). To further enhance modern computing and bring seamless connectivity to the world through interconnected smart devices, next-gen technology is needed. This technology is enabled by 5G, which offers fast speeds, low latency, and widespread coverage (Gupta et al., 2020). The growth of modern computing is also fueled by IoT innovations. Additionally, the application of blockchain technology in IoT can provide a decentralized, secure, and sensitive information in a public, transparent ledger that enables transactions to be checked by a network of possibly unreliable parties. (Reyna et al., 2018).

IoT is a rapidly growing technology that is being integrated into various markets, industries and daily life. It offers numerous applications, functions and services, improving the way we live and work (Lampropoulos et al., 2018). The utilization of IoT can be observed in healthcare, environment, smart cities, business, industry and infrastructure development (Souri et al., 2017; Souri et al., 2018). People's usage of IoT in different sectors drives its popularity and acceptance (Chettri & Bera, 2020). By studying the application of IoT, we can improve the technology and generate new ideas for future use (Tun et al., 2020). IoT enables communication between objects by transferring information, leading to limitless possibilities (Redhu et al., 2018; de Almeida et al., 2019).

I. *BACKGROUIND RESEARCH*

A. Innovative features in modern computing

The innovation in the supply chain system of IoT has resulted in improved functionality and processes, leading to various benefits such as increased efficiency, accuracy, real-time monitoring, better decision-making, cost reduction, and customer satisfaction (Cui, 2018). One of the major innovations in this field has been the implementation of Radio-Frequency IDentification (RFID) sensors and devices, which have had a significant impact on the physical communication layer of IoT, logistics, and robotics (Mezzanotte et al., 2021). Additionally, the integration of blockchain technology has brought new perspectives to the security, resilience, and efficiency of digital systems (Ahram et al., 2017). Moreover, the creation of Low Power Wide Area Networks (LPWANs), a brand-new category of wireless network made specifically for Internet of Things applications, allows for effective long-range communication while minimizing power usage and battery life (Chaudhari et al., 2020).

B. Current trends of IOT

IoT is currently being used in healthcare for wearable technology, telemedicine, smart biosensors, smart ambulances, and remote patient monitoring. (Wang et al., 2015).The improvement of public utility infrastructure through smart metering and smart-grid systems (Lloret et al., 2016) is another trend. The easy and affordable idea of smart houses (Park et al.,2017) and smart cities (Mohanty, et al., 2016) and the use of IoT for efficient health management through a smart gym (Zhao et al., 2015) are also prevalent trends. 5G is the next-gen wireless tech with improved speed and connectivity, IoT devices will be a big part of the 5G network (Ejaz et al., 2016). The growth of IoT is being propelled forward significantly by the development of 5G networks. (Wang et al., 2018).

C. Future trends of IOT

As current technologies like 4G, 3G, 2G, Wi-Fi , and Bluetooth have constraints for low power and low data rate devices, the future of IoT devices is heading toward 5G. (Marcus, 2015; Li et al., 2018; Díaz Zayas et al., 2017). 5G technology is seen as the solution to these limitations (Marcus, 2015). Blockchain technology is seen as a solution for privacy, security, and data integrity issues in smart homes (Moniruzzaman et al., 2020). Data management systems integrating IoT, big data, and cloud computing are improving city operations and quality of life (Soomro et al., 2019). The adoption of disruptive technologies such as IoT, big data, AI, and blockchain has the potential to accelerate the evolution of smart cities (Soomro et al., 2019).

D. Basic system security

The three main concerns for IoT data security are confidentiality, integrity, and availability (Mohanty et al., 2020). The security challenges present in different layers of IoT operations such as 6LoWPAN adaptation, transport, routing, and application (Granjal et al., 2015). Blockchain can be a key enabling technology for providing viable security solutions to IoT security problems.(Khan & Salah, 2018). Machine learning is an approach that enables intelligent computation and integration with IoT applications. It can be applied to process and analyze vast amounts of data, predict and alert for fires, and enhance system security. (Al-Garadi et al., 2020) . IoT and Cyber Physical Systems is simpler to secure than IoT, using conventional cryptographic techniques (Gunathilake et al., 2020). By implementing these solutions, individuals, organizations, and governments can help ensure the security of IoT devices and networks, and protect against cyber threats.

II. INTRODUCTION

This gadget is designed with the help of an Arduino using a servo motor that pushes the gear forward and back. When we scan our register card, there is a loop start of store programming in which the servo motor rotates 180 degrees, then the gear mechanism in it works, which opens the lock. In simple language, when a card is scanned, the condition given in the programming matches, then the command given in that condition becomes active, such that when the correct card is scanned, then the LED will display the door is opening then after some seconds the servo motor will rotate 180 degree and the door lock will be open but when an unregistered card is scanned then the condition of the wrong card will match which. The Wrong card will show on the LCD.

III. TECHNICAL DEVELOPMENT OF THE PRODUCT

This section outlines the necessary hardware components needed to implement the proposed solution for the system. To demonstrate the required connections between these components, Tinkercad was used to provide a clear and labeled diagram. Furthermore, a complete description of each component is presented to provide a comprehensive understanding of their roles in the system.

A. Hardware requirement

Here are some more details about each component:

1. Microcontroller (Arduino UNO): A microcontroller is a compact computing device integrated into a single chip. It is designed for managing specific tasks in embedded systems. In this case, the Arduino UNO microcontroller is used to execute the programmed code and control various functions related to the access control system.

2. RFID Module: An RFID (Radio-Frequency Identification) module is a device that uses radio waves to read and communicate with RFID tags or cards. In this context, it is employed to scan registered cards and compare their information with the programmed conditions.

3. LCD (Liquid Crystal Display): An LCD is a type of display technology that uses liquid crystals to create visual output. In this system, an LCD screen is used to provide visual feedback, such as displaying messages like "Wrong Card" or "Door Opening."

4. 5V Power Supply or Battery: A 5V power supply or battery provides a constant voltage output of 5 volts. In this setup, it may be used to power various components within the system, ensuring they receive a stable voltage.

5. Servo Motor: A servo motor is a rotary actuator that allows for precise control of angular position. In this system, it is employed to physically control the locking mechanism, rotating to open or close the door.

6. Door Lock: The door lock is a mechanical or electronic locking device that secures the door. In this context, the door lock is part of the access control system and is controlled by the servo motor based on the conditions programmed in the Arduino.

B. Component

The component diagram of my device and details discussion

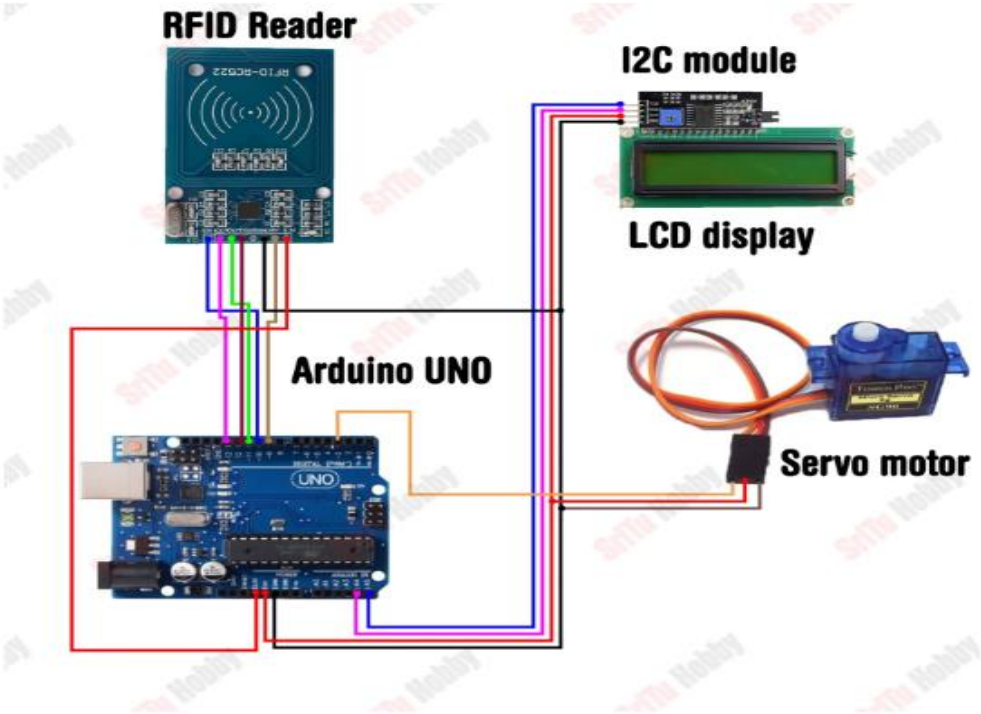


Fig.2. RFID-Based Digital Door Locking System

```
1| int outputPin = 3;
2| int triggerPin = 5;
3| int resetPin = 4;
4| void setup() {
5| pinMode(outputPin, OUTPUT);
6| pinMode(triggerPin, OUTPUT);
7| pinMode(resetPin, OUTPUT);
8| }
9| void loop() {
10|  digitalWrite(triggerPin, HIGH);
11|  delay(10);
12| digitalWrite(triggerPin, LOW);
13| if(analogRead(A0) >= 900) {
14| digitalWrite(resetPin, HIGH);
15| digitalWrite(outputPin, LOW);
16| } else {
17| digitalWrite(resetPin, LOW);
18| digitalWrite(outputPin, HIGH);
19| }
```

Fig.3. Arduino coding

IV. RFID-BASED DIGITAL DOOR LOCKING SYSTEM

Figure 5: Mechanism of Door Lock System

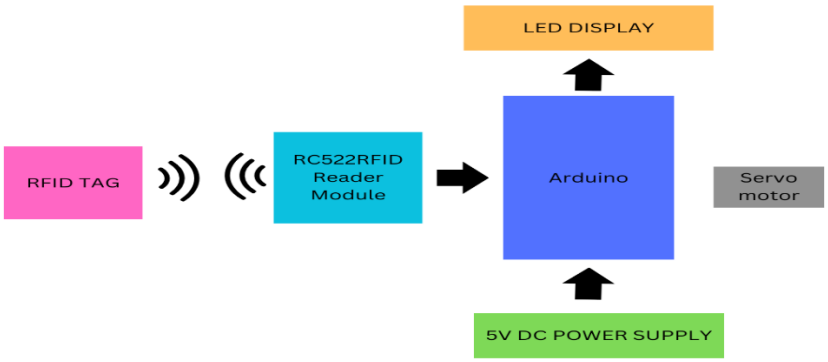


Figure 6: Block Diagram of RFID Door Lock System using Arduino

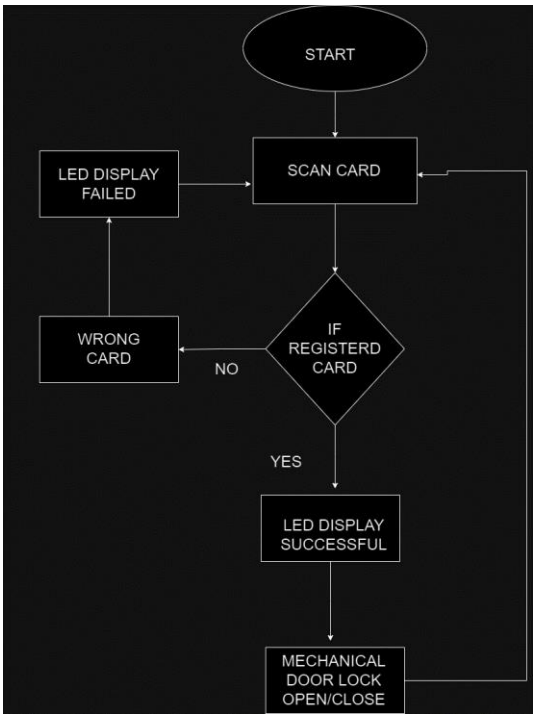


Figure 6: Flowchart Working Metho

V. SECURITY CONSIDERATION

Security is the practice of protecting systems, devices, and networks from unauthorized access, use, theft, damage, or disruption. This sections provides the details information about the consideration security

1. *Data Encryption*: Ensure that data transmissions between the RFID module, Arduino, and other system components are encrypted. This safeguards the communication process, preventing unauthorized access and maintaining the privacy of user information.

2. *Access Control*: Implement robust access control mechanisms within the Arduino code. This ensures that only authorized individuals can trigger the door-opening mechanism with registered cards. Unauthorized access attempts should be actively monitored and reported.

3. *Authentication Layer*: Develop a secure authentication layer within the system's code. This layer must verify the authenticity of registered cards and users before granting access. Strong authentication mechanisms should be employed to prevent bypassing the system.

4. *Firmware Security*: Safeguard the system's firmware. Ensure that the Arduino's code is protected against unauthorized modifications or tampering. Unauthorized changes to the programming can compromise the system's security.

5. *Software Updates and Patching*: Regularly update and patch the system's software to address known vulnerabilities. This includes keeping the Arduino code up to date and applying security patches as needed to maintain system integrity.

6. *User Education*: Educate system users on secure usage practices. They should be informed about how to handle registered cards securely, configure the system properly, and recognize and report any suspicious activities. Security awareness among users is vital for the overall system's integrity.

7. *Physical Security Measures*: Physically secure the access control system and its components. This may involve securing the Arduino and related hardware within a locked enclosure or mounting the system in a way that limits unauthorized access. Preventing physical tampering is essential for maintaining system security.

VI. CONCLUSIION

A. Further Enhancements:

1. *Multiple User Support*: Extend the system to support multiple registered cards or users. Store user information in a database and ensure that the Arduino can recognize and validate multiple cards. This would involve enhancing your code to manage a list of registered cards and their associated permissions.

2. *Security Logging*: Implement a security log to record every access attempt, including successful and unsuccessful ones. Log entries could include the timestamp, user ID, and the result (successful or denied access). This can help in monitoring and auditing access.

3. *Remote Access Control*: Connect the Arduino to a network module (e.g., Wi-Fi or Ethernet shield) to allow remote access control. This could involve building a smartphone app or a web interface to manage and monitor access.

4. *Voice or Keypad Entry*: Implement an additional method of entry for users without RFID cards, such as a keypad or voice recognition system. This enhances flexibility and usability.

5. *Battery Backup*: Ensure that the system can operate on battery power in case of a power outage. Implement a battery backup system to maintain access control functionality even when the primary power source is disrupted.

6. *Access Scheduling*: Add a feature for scheduling access permissions. Users or administrators can set specific time windows during which access is allowed or denied for certain cards.

7. *Intrusion Detection*: Incorporate sensors, such as motion detectors or door contact sensors, to detect unauthorized entry attempts or break-ins. The system can respond by sounding an alarm or notifying the authorities.

8. *User Management Interface*: Create a user-friendly interface for administrators to add, remove, or modify user profiles and access permissions, preferably through an LCD or a remote control app.

9. *Biometric Authentication*: For enhanced security, consider integrating biometric authentication methods like fingerprint or facial recognition alongside RFID card access.

B. Additional Programming:

To implement the above enhancements, we need to extend your programming. Here's a general outline of what you might need to do:

1. *User Database*: Create a structured database to store user information, including user IDs, RFID card data, access permissions, and other relevant details.

2. *Network Integration:* If implementing remote access control, we need to code the communication between the Arduino and the remote interface, ensuring data security.

3. *Logging*: Write code to log access attempts, including timestamps, user IDs, and access outcomes, to a storage medium or display the logs on the LCD screen.

4. *Power Management*: Implement code to monitor the power source (battery or main supply) and switch between them as needed to ensure uninterrupted operation.

5. *Scheduling*: Develop code to manage access schedules, allowing users or administrators to define access time periods.

6. *Security Alerts*: Create code to trigger alarms or notifications in the event of a security breach, and ensure that it reacts appropriately to unauthorized entry attempts.

7. *Biometric Integration*: If adding biometric authentication, include the necessary libraries and code to read and verify biometric data.

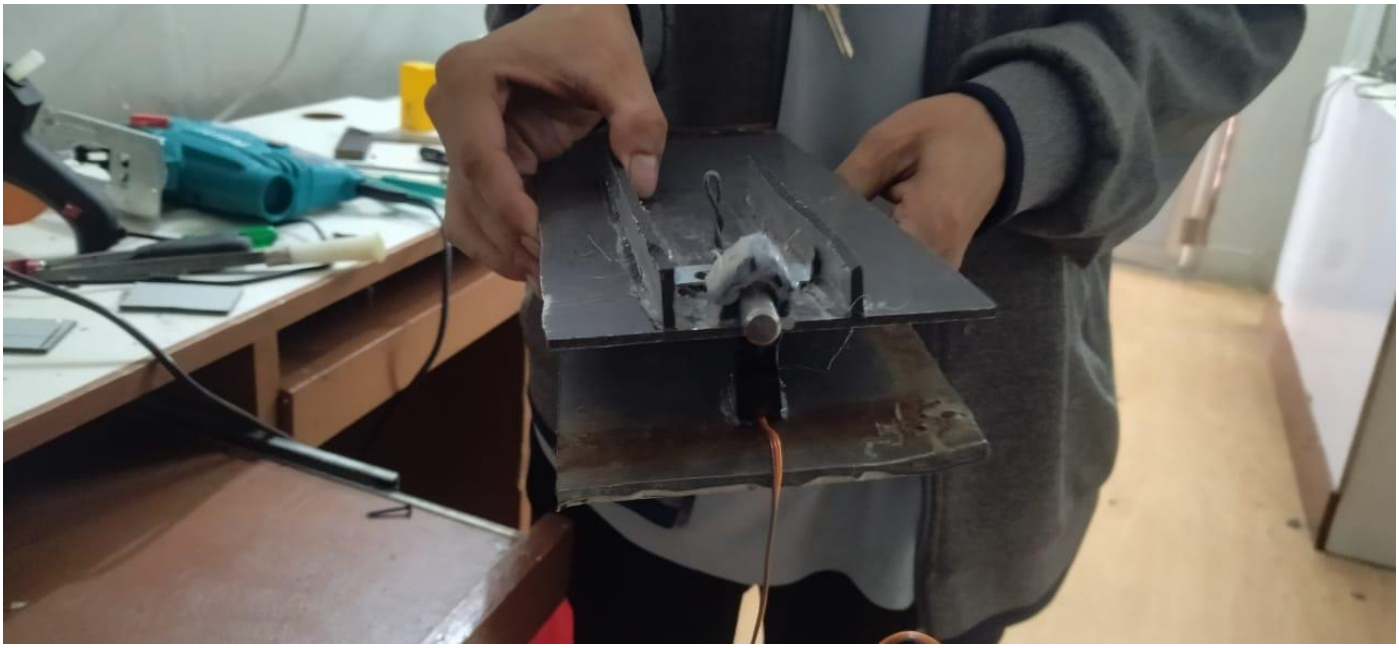
8. User Management Interface: Design a user-friendly interface to manage user profiles, including adding, removing, and modifying user information, and granting or revoking access permissions.

PROGRESS REPORT

RFID-Based Digital Door Locking System

Sudeep fullel and Dikshant Madai

2023/10/12



I. Executive Summary

As of the report date, we present an update on the progress of the RFID-Based Digital Door Locking System project, detailing major accomplishments, current status, and the key challenges faced. Due to unavailability, the project has adapted to using IR sensors in place of RFID technology for hardware development. Despite initial hurdles, we have made significant strides in hardware design and are now in the testing phase. The integration of IoT components has also been addressed, with a fiberboard enclosure selected for housing. Moreover, we discuss the functioning of the gadget, highlighting its recognition of registered and unregistered cards. Lastly, the report delves into the security measures in place, including assessments and improvements.

II. Project Objectives

List the specific objectives and goals that were set for the RFID-Based Digital Door Locking System project.

- Objective 1: Collect and Connect all the Required Component and hardware for our Prototype
- Objective 2: Design of RFID-Based Digital Door Locking System project's
- Objective 3: Planning for the final designing of RFID-Based Digital Door Locking System project's

III. TECHNICAL DEVELOPMENT OF THE PRODUCT

This section outlines the necessary hardware components needed to implement the proposed solution for the system. To demonstrate the required connections between these components, Tinkercad was used to provide a clear and labeled diagram.

Furthermore, a complete description of each component is presented to provide a comprehensive understanding of their roles in the system.

A. Hardware requirement

Here are some more details about each component:

1. Microcontroller (Arduino UNO): A microcontroller is a compact computing device integrated into a single chip. It is designed for managing specific tasks in embedded systems. In this case, the Arduino UNO microcontroller is used to execute the programmed code and control various functions related to the access control system.

2. IR Sensor: IR sensor acts as a trigger for the system. When it detects an obstacle within a certain range (like someone approaching the door), it activates the programmed response, which includes opening the door using the servo motor and displaying relevant information on the LCD screen.

3. LCD (Liquid Crystal Display): An LCD is a type of display technology that uses liquid crystals to create visual output. In this system, an LCD screen is used to provide visual feedback, such as displaying messages like "Wrong Card" or "Door Opening."

4. 5V Power Supply or Battery: A 5V power supply or battery provides a constant voltage output of 5 volts. In this setup, it may be used to power various components within the system, ensuring they receive a stable voltage.

5. Servo Motor: A servo motor is a rotary actuator that allows for precise control of angular position. In this system, it is employed to physically control the locking mechanism, rotating to open or close the door.

6. Door Lock: The door lock is a mechanical or electronic locking device that secures the door. In this context, the door lock is part of the access control system and is controlled by the servo motor based on the conditions programmed in the Arduino.

B. Component

The component diagram of my device and details discussion

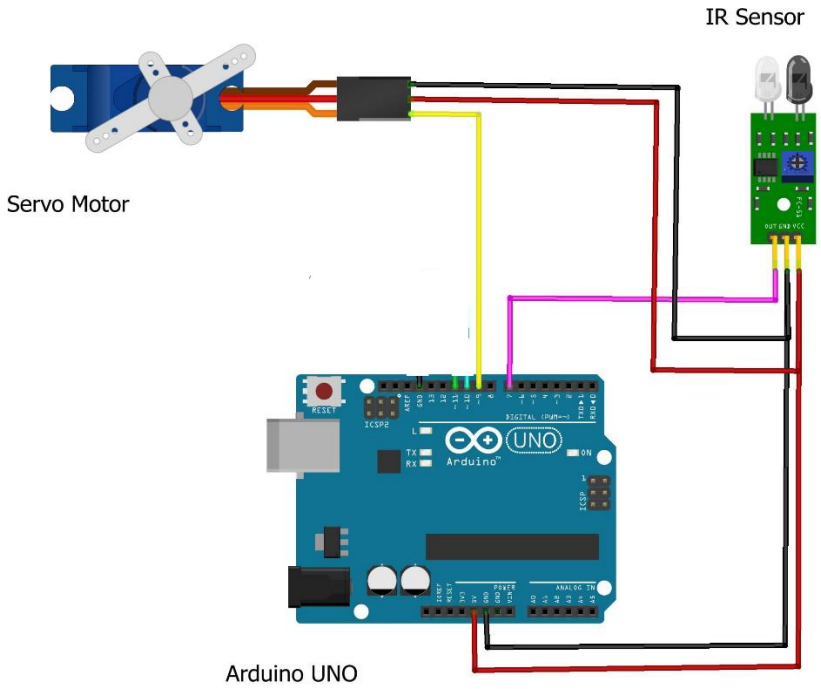


Figure: IR Based *Digital Door Locking System*

```
1| int outputPin = 3;
2| int triggerPin = 5;
3| int resetPin = 4;
4| void setup() {
5| pinMode(outputPin, OUTPUT);
6| pinMode(triggerPin, OUTPUT);
7| pinMode(resetPin, OUTPUT);
8| }
9| void loop() {
10|  digitalWrite(triggerPin, HIGH);
11|  delay(10);
12| digitalWrite(triggerPin, LOW);
13| if(analogRead(A0) >= 900) {
14| digitalWrite(resetPin, HIGH);
15| digitalWrite(outputPin, LOW);
16| } else {
17| digitalWrite(resetPin, LOW);
18| digitalWrite(outputPin, HIGH);
19| }
```

Fig.3. Arduino coding

Figure 5: Mechanism of Door Lock System

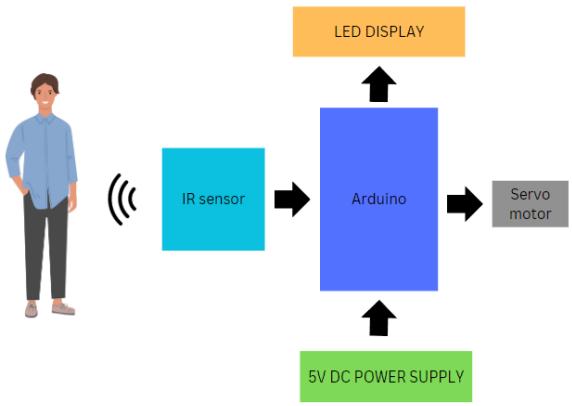


Figure 6: Block Diagram of RFID Door Lock System using Arduino

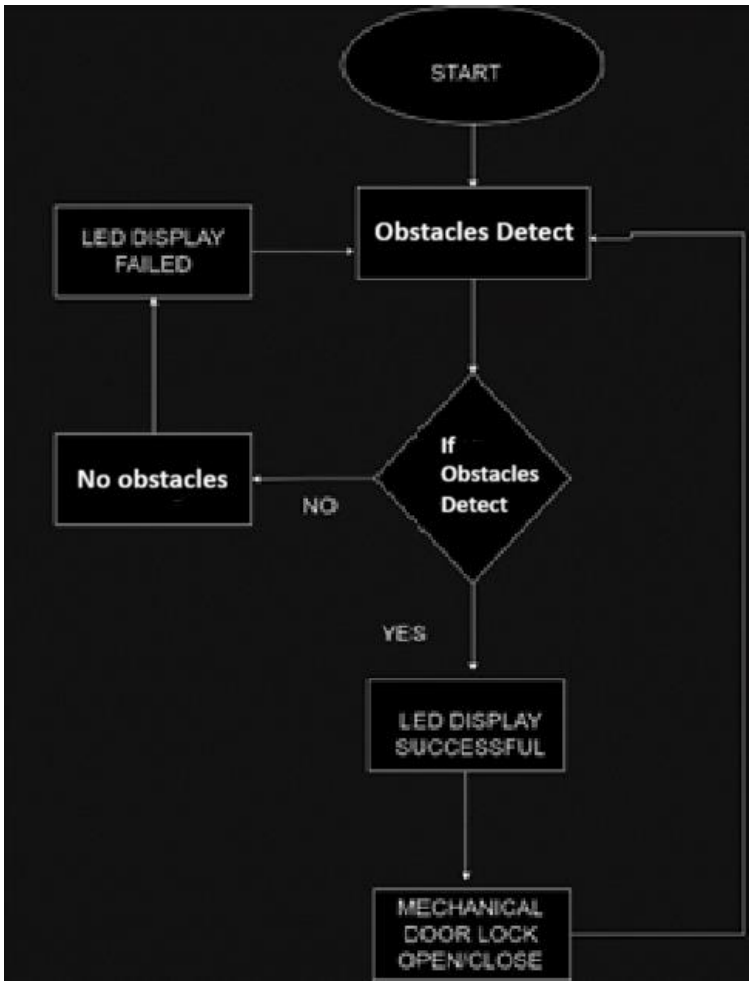


Figure 6: Flowchart Working Metho

IV. Progress Update

A. Hardware Development

1. RFID Hardware Development Update:

Due to the unavailability of RFID technology, we have employed IR (Infrared) sensors as an alternative solution for our project. These sensors have become a crucial component of our hardware development.

2. Challenges Faced and Solutions Applied:

- Availability of RFID Technology: The primary challenge we faced was the unavailability of RFID technology, which was initially planned for our project. In response, we conducted thorough research and determined that IR sensors could serve as a viable alternative for our purposes.

- Integration into the Hardware: Integrating IR sensors into our hardware posed a challenge due to differences in technology and compatibility. To address this, we consulted with experts and modified our hardware design to accommodate IR sensor components.

3. Status of the Hardware Prototype:

At present, we have successfully completed the initial design of our hardware prototype, which incorporates IR sensors. We have made significant progress in this aspect of development, and our prototype is in the testing phase. This phase includes testing the functionality and accuracy of the IR sensors in various scenarios.

4. Case and Housing for IoT Components:

We have identified an appropriate housing solution for our IoT (Internet of Things) components. To fit our entire mechanism and IoT components, we have chosen to use a fiberboard enclosure. This enclosure offers durability and protection to the internal hardware components while allowing for efficient communication between the IR sensors and the central control unit for our prototype design.

B. IR Integration**

This gadget is designed with the help of an Arduino using a servo motor that pushes the gear forward and back. When the IR Sensor detect the obstacles there is a loop start of store programming in which the servo motor rotates 180 degrees, then the gear mechanism in it works, which opens the lock. In simple language, when IR Sensor detect the obstacles, the condition given in the programming matches, then the command given in that condition becomes active, such that when the obstacles has detected in the certain given range, then the LED will display the door is opening then after some seconds the servo motor will rotate 180 degree and the door lock will be open but when an obstacles has not detect then the condition will not match the door wont open.

Discuss any integration difficulties and how they were resolved.

C. Security Measures

Security measures in place for safeguarding the system include encryption and authentication protocols to prevent unauthorized access. Regular security assessments have been conducted to identify vulnerabilities and enhance the system's overall security. Measures such as a temporary lockout mechanism have been implemented to protect against multiple failed access attempts. These security features continue to be refined to ensure the system's integrity and reliability.

D. Testing and Quality Assurance**

- Provide an overview of the testing process and the results obtained.
- Report any identified bugs or issues and how they were addressed.

D. User Feedback

- Summarize the user feedback received during the testing phase.
- Describe any modifications made based on user suggestions.

V. Challenges and Mitigations

Identify the challenges or obstacles encountered during the project and detail the steps taken to overcome them.

V. Next Steps

Discuss the upcoming tasks and milestones essential to complete the project. Include a timeline if available.

VI. Budget and Resource Allocation

Offer an overview of the project's budget, expenses incurred so far, and how resources have been allocated.

VII. Conclusion

Summarize the progress report, emphasizing the project's current status and the path forward.

VIII. Attachments

Include any relevant documents, diagrams, or images that support the progress report.

Photos