International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 5, May 2025)

RFID Door Lock

[1]Shashank Shrivastava, [2]Shweta Choudhary, [3]Prof. Rajdeep Shrivastava
[1,2]Student, Department of Electronics & Communication Engineering, LNCTE, Bhopal, India
[3]Guide, Department of Electronics & Communication Engineering, LNCTE, Bhopal, India

***Abstract*— The RFID (Radio Frequency Identification) Door Lock System is a smart, technology-driven solution designed to enhance security and improve access control for residential, commercial, and industrial environments. This project integrates RFID technology with microcontroller-based systems to create a user-friendly, reliable, and scalable locking mechanism. The system consists of an RFID reader, a set of programmable RFID tags/cards, a microcontroller unit, and an electromechanical locking device. The system functions by scanning RFID tags/cards, each embedded with a unique identifier. Upon scanning, the RFID reader transmits the tag's data to the microcontroller, which authenticates it against a pre-programmed database. If the tag is authorized, the system activates the lock to grant access. Unauthorized tags trigger a security response, such as sounding an alarm or notifying the user. This project highlights features such as low power consumption, durability, and minimal maintenance, making it a viable alternative to traditional key-based systems. Additionally, the system offers advanced functionalities, including easy user management, the ability to add or remove tags, and the potential for integration with IoT platforms for remote monitoring and control via smartphones or other devices. The RFID Door Lock System combines security, convenience, and adaptability, addressing the increasing demand for smart security solutions in modern society. The project's development underscores the importance of data encryption, efficient authentication protocols, and user-friendly interfaces, providing a foundation for future advancements in access control technologies.**

***Keywords*—Water, Dispenser, Battery, Machine.**

I. INTRODUCTION

In today's rapidly evolving technological landscape, the demand for efficient, secure, and user-friendly access control systems has become increasingly significant. Traditional lock-and-key mechanisms, while still widely used, are often vulnerable to issues such as key duplication, loss, or damage. This has led to the development of more advanced security solutions, including electronic and smart locking systems. Radio Frequency Identification (RFID) technology has emerged as a highly effective approach to modern access control. An RFID door lock system uses electromagnetic fields to identify and authenticate individuals through RFID tags or cards. These tags are embedded with unique identifiers, making unauthorized duplication nearly impossible. The system eliminates the need for physical keys, enhancing convenience while maintaining robust security. The RFID door lock system consists of several core components: an RFID reader, which scans tags/cards; a microcontroller, which processes and verifies the scanned data; and an electromechanical lock, which is activated upon successful authentication. Additional features, such as integration with mobile applications or IoT devices, can further enhance functionality, offering users remote access control and monitoring capabilities.

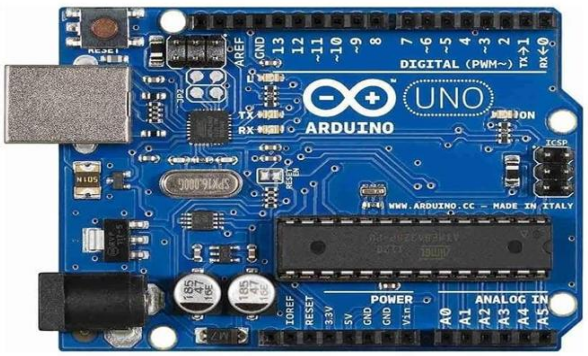

Figure 1: Arduino UNO Board

This introduction provides an overview of the need for secure and efficient access control systems, the principles behind RFID technology, and the objectives of developing an RFID door lock system. The project aims to demonstrate the potential of RFID technology to transform traditional access methods into seamless, high-security solutions for modern applications. Security and convenience are fundamental requirements in modern living and working environments. Traditional locking mechanisms, which rely on physical keys, have served as the primary means of access control for centuries. However, these systems have notable limitations, including vulnerability to key loss, duplication, and wear-and-

tear. As society increasingly prioritizes smart and efficient technologies, electronic solutions like RFID (Radio Frequency Identification) systems have gained popularity for their enhanced security and user-friendly.

The RFID door lock system is an innovative access control solution that leverages RFID technology to provide a secure, reliable, and flexible alternative to conventional locks. This system employs RFID tags or cards as virtual keys, each carrying a unique identifier that communicates with an RFID reader. Upon scanning a tag, the reader sends the data to a microcontroller, which validates the tag's authenticity. If the tag matches the pre-approved database, the system grants access by unlocking the door. Unauthorized attempts are flagged, ensuring high levels of security.

II. LITERATURE SURVEY

RFID is a contactless communication system that uses radio waves to transmit data between an RFID tag (or transponder) and an RFID reader. The tag contains stored information, usually a unique identifier (UID), which is transmitted to the reader when within range. This technology is categorized into three types: low-frequency (LF), high-frequency (HF), and ultra-high-frequency (UHF) RFID. The choice of frequency affects the communication range, data transfer rate, and environmental performance. Passive RFID tags rely on the energy emitted by the reader for power, while active tags have their own power source and can transmit signals over longer distances.

One of the most prominent applications of RFID technology is in access control systems, including RFID door locks. These systems use RFID tags embedded in cards, fobs, or wristbands for user identification. When a valid tag is detected by the RFID reader, it triggers the lock to open. These systems provide advantages over traditional mechanical locks, such as greater convenience, faster access, and no need for physical keys. RFID-based access control systems are used in various settings, including residential buildings, offices, hospitals, and high-security environments.

Security is a significant concern in RFID systems due to the potential for data interception, unauthorized access, and tag cloning. Several studies have highlighted vulnerabilities in basic RFID systems, where communication can be intercepted or manipulated by attackers using devices to eavesdrop or clone RFID tags. This risk has led to the development of advanced security measures, such as encryption and mutual authentication. In high-security applications, the use of AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) encryption algorithms ensures that communication between the RFID tag and reader is secure. Techniques like rolling codes, hash-based authentication, and secure boot processes are also being integrated to enhance security and prevent unauthorized duplication of RFID tags.

Simulation plays a crucial role in designing and testing RFID-based systems, particularly door locks. Tools like Proteus and MATLAB are used to simulate RFID interactions, including tag-reader communication, encryption, and the response times of the locking mechanisms. These simulations help identify potential weaknesses in system design, such as the distance between the reader and the tag, environmental interference, and power consumption. Simulation also aids in testing security protocols to ensure they are robust against attacks like signal jamming, data interception, and unauthorized access.

RFID technology is increasingly being integrated into the Internet of Things (IoT), leading to smarter security systems that can communicate with other devices and cloud-based platforms. For instance, RFID-based door locks can be part of a larger smart home system, allowing for remote access, monitoring, and integration with other sensors like motion detectors or cameras. This integration increases the convenience and flexibility of RFID systems while improving the ability to manage access and monitor security remotely.

The development of RFID door locking technology can be traced back to the foundational advancements in radio frequency identification (RFID) technology, which began in the mid-20th century. The concept of RFID originated in the 1940s, with the development of radar systems during World War II, which allowed for the identification of friendly aircraft using transponder technology. In 1948, Harry Stockman's influential paper on "Communication by Means of Reflected Power" laid the groundwork for what would later become RFID technology. Throughout the 1950s and 1960s, passive RFID systems were developed, which used external radio waves to power tags, and these early systems found limited use in inventory management and livestock tracking. It wasn't

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 5, May 2025)

until the 1970s and 1980s that RFID technology began to evolve, particularly with the introduction of more reliable and compact tags, making them suitable for commercial applications, including vehicle tracking and toll collection.

By the late 1990s, RFID technology saw further refinement, with the development of more secure and efficient passive tags, which did not require a battery to function. This period marked a significant shift, as RFID began being explored for applications beyond logistics, such as in security and access control systems. The integration of RFID into door locking technology began in the early 2000s, offering a contactless, more secure alternative to traditional mechanical locks. The key advantage of RFID systems in access control was their ability to allow for quick, convenient, and secure user authentication through RFID tags or cards. Over time, RFID locks became increasingly sophisticated, incorporating features like remote management via mobile apps, integration with smart home ecosystems, and enhanced security protocols like encryption. Today, RFID door locking technology is widely used in various sectors, including residential, commercial, and industrial applications, offering a secure, reliable, and scalable solution for access control.

III. WORKING

The system is composed of three major modules. The microcontroller module consists of the Arduino Uno R3 microcontroller. The RFID module serves as the input of the microcontroller, as the registered card required to open the door must be scanned into the system through the module. The gear mechanism module controls the mechanical action (opening and closing) of the door. It includes a servo motor. The mechanism of this door lock system makes is explained in figure 1. There are main four processes by which this gadget works. These four blocks are namely RFID Scanner, Microcontroller, Servo Motor, and Mechanical Door. First, the RFID tag will be scanned by RFID scanner, then the command will go to the microcontroller, The microcontroller will check that if the card is registered or not, then the command will go to the servo motor, according to which programming the servo motor will be rotated 90° so that the mechanical door lock will work.

Firstly, the door lock system will start, and the scanning process occurs, if the card is registered previously then the command will proceed otherwise the WRONG CARD message appeared with the Red LED blinks 2 times in 1 second and buzzer 2 times in 1 second and again the command scanning process will start, If the card is registered, the Red LED will be blink once for only 500 microseconds and buzzer beeps 1 time for 500 microseconds and the command will execute into the mechanical door lock system and the door lock will be open. When the door lock is open, the command will run again and the scanning process starts, but now the door lock will be closed.

Data Transmission:

Data transmission in an RFID-based door lock system involves communication between the RFID tag (transponder), the RFID reader, and the system that controls the door lock. This process ensures that only authorized users can access the system. Data Transmission Process in RFID Door Locks: RFID Tag (Transponder) and Reader Communication: • RFID Tag: The tag typically holds a unique identifier (UID), which can be either stored in the memory of a passive or active RFID tag. Passive tags rely on the energy from the RFID reader's electromagnetic field, while active tags have a battery to power them. • RFID Reader: The reader emits an electromagnetic signal to power up the RFID tag and request its data. Once the tag is energized, it transmits its stored data (usually the UID or other encrypted data) back to the reader. Reader to Lock System Communication: • Signal Processing: The reader processes the data it receives from the RFID tag (typically the UID or encrypted data). The data is then transmitted to the door lock system's controller (either locally or over a network). • Data Transmission Protocol: Depending on the system's design, the reader communicates with the controller via serial protocols (e.g., UART, I2C, SPI), or via wireless protocols (e.g., Bluetooth, Wi-Fi) in more advanced systems. If the system uses encryption, the data can be transmitted securely using protocols like AES or RSA for data confidentiality.

Verification by the Lock Controller:

• Access Control Database: The controller compares the received UID or data against an access control list (ACL) stored in its database (local or remote). This database determines whether the tag belongs to an authorized user. • Decision Making: If the tag's data matches an authorized entry, the controller sends a signal to the electronic locking mechanism to unlock the door. In some systems, additional steps like two-factor authentication (PIN + RFID) may be required.

Feedback to the User:

• Access Granted or Denied: The system may signal the user with feedback such as a green light, a beep, or a display message to indicate whether access was granted or denied. If

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 5, May 2025)

access is granted, the door is unlocked, allowing the user to enter.

IV. TESTING AND SIMULATION

Testing: Testing an RFID door lock system involves ensuring that all components work as expected and the system remains secure under different conditions. Functional testing includes verifying that the RFID reader can properly detect authorized and unauthorized RFID tags, unlocking the door only for valid tags. It also involves testing the locking mechanism to ensure it engages when the door is closed and that the system responds promptly to unlocking commands. In security testing, the focus is on verifying the encryption of communication between the RFID tag and reader. This involves testing for vulnerabilities, such as data interception or unauthorized tag cloning, and ensuring the system uses secure protocols (e.g., AES or RSA) for data transmission. Additionally, the system's ability to handle multiple users is tested by enrolling several tags and checking that only authorized tags can unlock the door. Testing also includes evaluating the system's response to environmental factors, like signal interference or power failure, to ensure reliable operation under real-world conditions. This comprehensive testing ensures both the functionality and security of the RFID door lock system. Testing an RFID Door Lock system involves evaluating both the hardware and software components to ensure they function properly, securely, and reliably. Proper testing is essential to confirm the system's performance, security, and usability.

Simulation: Simulation in an RFID door lock system involves using software tools to model and test the behavior of the RFID components before physical implementation. This allows developers to verify the functionality, security, and performance of the system without the need for hardware. Simulation typically includes modeling the communication between the RFID reader and tags, ensuring that valid tags are recognized and the door lock mechanism is triggered appropriately. Tools like Proteus or MATLAB can simulate the interactions between the RFID reader, the controller, and the lock, testing scenarios such as valid and invalid tag scans, encryption protocols, and response times. Additionally, security simulations can check for vulnerabilities like signal jamming, data interception, and unauthorized access attempts. This helps in refining the system design, identifying potential issues, and ensuring the system works as intended under various conditions. Overall, simulation in RFID door locks is a critical step to optimize the system's reliability and security before deploying the physical setup. Further simulation in an RFID door lock system extends to more detailed aspects of system performance, user interaction, and security. For example, advanced simulations can include testing the integration of RFID technology with other security features like PIN codes or biometric authentication, simulating how these features interact and verify users. In such cases, the simulation tools model multi-factor authentication scenarios to ensure the system only grants access to authorized individuals. Moreover, the simulation can focus on real-world environmental factors that could affect RFID communication, such as interference from metal objects, electronic devices, or extreme weather conditions. This is especially critical in scenarios where the RFID system is used outdoors or in areas with potential signal obstructions. By simulating these conditions, developers can identify areas of vulnerability, optimize tag-reader distance, and adjust antenna configurations to ensure reliable communication. Another important aspect of RFID lock simulation is power failure or reset scenarios. Simulations can test the system's resilience to power loss by ensuring the lock reverts to a secure state or properly performs recovery procedures, such as reverting to the last known state (locked or unlocked). Testing the battery life and energy consumption of passive RFID tags and readers is also crucial, especially for systems relying on low-energy, battery-operated devices.

Figure 2: RFID Door Lock

V. CONCLUSION

The use of the Arduino UNO microcontroller in this project allows design simplicity, therefore, the project can be achieved in a shorter time than other technologies previously employed. And this door lock system is also very secure and saves the information of people coming and going. RFID technology has proven to be a powerful and versatile solution

in various applications, particularly in access control systems such as RFID door locks. It offers significant advantages in terms of convenience, speed, and security compared to traditional mechanical locks and key systems. RFID systems provide contactless identification, allowing for quick and seamless access while reducing the risk of physical wear and tear on locking mechanisms. The integration of encryption and advanced security protocols further enhances the safety of RFID door lock systems, protecting against unauthorized access and tampering. Overall, RFID technology continues to evolve, with advancements in security, energy efficiency, and integration with other smart technologies, making it an ideal choice for modern access control and security systems. As it becomes increasingly integrated with IoT and smart home devices, the future of RFID promises even more innovative applications, offering greater convenience and enhanced security in various fields, from personal access management to large-scale enterprise solutions.

REFERENCES

1. M. T. Nguyen and H. C. Nguyen, "Design of an RFID-based door access control system using Raspberry Pi and Python," 2020 IEEE International Conference on System Science and Engineering (ICSSE), Hanoi, Vietnam, 2020, pp. 124–128.

2. A. Sharma, S. Verma, and V. Mishra, "Development of a smart door locking system using RFID and cloud services," 2020 IEEE International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 1130–1134.

3. R. R. Manjula, N. N. Nayak, and P. B. Raikar, "IoT-based smart door locking system using RFID and NodeMCU," 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 2019, pp. 305–309.

4. D. Y. Patil and M. D. Ingle, "Design and implementation of RFID-based security system for doors," 2019 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bengaluru, India, 2019, pp. 221–225.

5. S. Bhardwaj and A. S. Gautam, "RFID based smart security and access control system using Arduino and GSM module," 2018 IEEE 8th International Advance Computing Conference (IACC), Greater Noida, India, 2018, pp. 208–213.

6. A. S. Bhosale and S. B. Patil, "Smart RFID based door lock system using Arduino," 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 2018, pp. 102–105.

7. P. S. Suhasini, M. D. Kumar, and R. Hariprasath, "RFID based door access control system," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 2017, pp. 542–546.

8. M. A. S. Kamal and M. R. Islam, "RFID based home security system with SMS alert using Arduino and GSM," 2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), Dhaka, Bangladesh, 2016, pp. 1–5.