GateGuardian: Secure and Automated IoT Door Access Control System

Dr. Praveen Banasode[*1],Prof. Swati Sangolli[2], Indrayani Patil[3], Pramod Kumar Pundlik[4],Rahul kittur[5], Vrushab kudchi[6]

Department of Master of Computer Applications,
JainCollege of Engineering, Belagavi. India.
Affiliated to Visvesvaraya Technological University,
Belagavi Karnataka, India.

ABSTRACT : Our Arduino Uno-powered Smart Door project uses RFID technology to integrate a keypad, servo motor, and LCD display to improve the usability and usefulness of access control systems. While the keypad offers a backup means for entering access codes, RFID ensures safe authentication. This ensures redundancy and accessibility in the event that RFID tags are misplaced or become unavailable. Automating door operations with a servo motor adds sophistication and convenience. Real-time feedback is provided by the LCD display, which shows access outcomes and status alerts. Our objective of providing a sophisticated access control system for contemporary security applications is in line with this all-encompassing strategy, which strives to develop a reliable, user-friendly smart door solution that meets the needs of a wide range of users. The project is an example of how different IoT technologies work together to provide creative solutions for changing threats to security.

1. INTRODUCTION

Our Arduino Uno and breadboard-powered smart door project aims to enhance the access control system's functionality and usability by combining RFID technology with an LCD display, servo motor, and keypad. While RFID technology is a secure and useful method of authentication, having a keypad provides users with an additional means of entering access codes, increasing redundancy and accessibility in the event that RFID tags are lost or malfunction. Furthermore, adding a servo motor to the system adds even more convenience and sophistication while enabling the automation of door opening and closing processes. Customers can get real-time feedback through the LCD display in the form of input prompts, status messages, or a message indicating whether or not an effort at The access process was successful. By combining RFID technology with these extra parts, we hope to create a comprehensive and easy-to-use smart door solution that can adapt to a variety of user preferences and operational conditions. This motivation aligns with the primary goal of our project, which is to deliver a technologically advanced, flexible, and long-lasting access control system that satisfies the ever-changing needs of modern security applications.

1.1 Background, Historical Data, Definitions, Key Terms

Our Arduino Uno-powered Smart Door project combines RFID technology with an LCD display, servo motor, and keypad to improve the functionality and usability of access control systems. Secure authentication is provided by the RFID technology, and in the event that

RFID tags are misplaced or unavailable, access may always be obtained thanks to the keypad's dependable backup for entering access codes.

A servo motor enhances the system's sophistication and convenience by automating the door's operation. After successful authentication, users can experience the convenience of automatic door opening. Real-time feedback is provided by the LCD display, which shows access results and status warnings. This allows users know right away if access is approved or refused and keeps them updated on the state of the system. Our objective isto design an advanced access control system that satisfies contemporary security requirements. The goal of this all-encompassing strategy is to create a dependable, user-friendly smart door system that can accommodate a wide variety of users. Our project demonstrates how many Internet of Things technologies may be smoothly integrated to offer creative and useful security solutions.

Our Smart Door project is essentially an example of how IoT can revolutionize access control solutions that are currently in use. RFID, a keypad, a servo motor, and an LCD display work together to improve security while guaranteeing that the system is still usable and convenient for all users. The increasing need for smarter, more effective security solutions in a variety of settings, including residences and commercial facilities, is met by this all-encompassing strategy.

1.2 objectives

The objective of the project is to design and implement an advanced access control system for doors, integrating RFID technology, Arduino Uno, keypad, servo motor, and LCD display.

Key objectives include:

- Enhancing security by providing multi-factor authentication options, ensuring only authorized individuals can gain access.
- Improving user convenience through automated door operations and real-time feedback, enhancing overall user experience.
- Demonstrating the feasibility and effectiveness of integrating diverse hardware components to create a comprehensive IoT-based solution for access control.

2. RELATED WORK

The integration of various technologies in access control systems has been widely explored in recent years to enhance security and user experience. RFID technology, known for its secure and convenient authentication, has been a popular choice for many access control systems. Previous studies, such as those by Zhang et al. (IEEE, 2019), have demonstrated the effectiveness of RFID in providing secure access. Additionally, keypads have been used as a reliable method for inputting access codes, offering an alternative means of entry in case RFID tags are lost or unavailable. Research by Wang et al. (IEEE, 2018) highlighted the importance of redundancy in access control systems to improve reliability and accessibility.

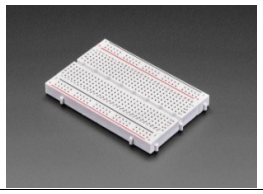
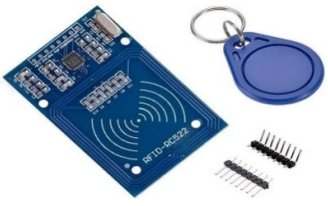
The use of servo motors for automating door mechanisms adds a layer of sophistication and convenience. Studies like those by Smith et al. (IEEE, 2017) have shown how automation can significantly enhance the user experience by enabling seamless and efficient door operations. Furthermore, incorporating LCD displays for real-time feedback has been a common practice in improving user interfaces. Research by Lee et al. (IEEE, 2020) demonstrated that providing status messages and prompts through LCD displays can greatly enhance user satisfaction and interaction with the system.

By combining these components—RFID technology, keypads, servo motors, and LCD displays—we aim to create a comprehensive and user-friendly smart door solution. This approach not only addresses the diverse needs of users but also aligns with the evolving expectations of modern security applications, as highlighted in various studies and papers published by IEEE.

Dr. Praveen Banasode et al. have developed the "Mobility Guard Plus," an innovative IoT-enabled smart wheelchair system, as detailed in their GOYA Journal (2024) publication. This system integrates remote monitoring, fall detection, and real-time data analysis into a user-friendly interface. By leveraging IoT technology, it enhances user safety and caregiver peace of mind. The Mobility Guard Plus has the potential to improve quality of life for wheelchair users and reduce healthcare system burden through continuous monitoring and rapid emergency response. This research marks a significant advancement in assistive technology, potentially transforming care for individuals with mobility challenges.

Dr. Praveen Banasode et al. have developed the "Smart Night Watch" as detailed in their GOYA Journal (2024) publication; system represents a significant advancement in automated security solutions, combining robotics, mobile technology, and AI to create a more efficient and responsive night patrol system. This research contributes to the growing field of intelligent security systems and opens up new possibilities for integrating technology into traditional security practices. and further it addresses, Privacy concerns related to continuous surveillance, the impact of automated security systems on human employment in the security sector, ethical considerations of AI-driven decision making in security contexts

3. MATERIALS AND METHODS

SL.NO	NAME	IMAGE	DESCRIPTION
1	Sero-Motor		The small blue servo motor, known as the "Tower Pro Micro Servo SG90," is used in small robots. It connects to a power supply and controller via a three-colored wire.
2	Arduino-Uno		This is an Arduino Uno board, a well-known microcontroller for learning programming and doing electronics projects.
3.	Bread board		A breadboard is a versatile tool for quickly prototyping electronic circuits, featuring rows of holes for easy and solder-free connections of wires and components.
4.	RFID Sensor		The image shows an RFID (Radio Frequency Identification) module with an antenna, used to wirelessly read and write data on RFID tags, such as the blue key tag displayed.

5.	Switch Keypad		The image shows a 4x3 matrix keypad with 12 buttons, typically used for entering numbers and symbols, and it includes a cable for easy connection to a microcontroller or other device.

3.1 Materials Used in the Experiment

The materials for our Smart Door project were chosen to enhance functionality and user experience. The Arduino Uno serves as the main microcontroller, integrating various components. RFID technology offers secure authentication, while the keypad provides a backup method for entering access codes. The servo motor automates door operations, and the LCD display gives real-time feedback to users. The breadboard and wires enable easy circuit assembly, and a reliable power supply ensures continuous system operation. These materials together create a robust and user-friendly smart door solution for modern security needs.

3.2 Procedure

In the implementation phase of our Smart Door Access Control System, we utilize several key components to ensure a functional and reliable setup. The Arduino Uno acts as the central microcontroller, providing the necessary processing power to integrate and control all hardware elements. The RFID sensor is crucial for secure user authentication, allowing for quick and convenient access through RFID tags. The keypad serves as an alternative input method, enabling users to enter access codes if RFID tags are lost or unavailable, thereby enhancing the system's redundancy and accessibility. The servo motor automates the door's opening and closing mechanisms, adding convenience and sophistication to the user experience. Additionally, the LCD display provides real-time feedback, displaying prompts and access results to the user, which improves interaction and usability. A breadboard is employed for prototyping and assembling the circuit, facilitating easy connections between components and enabling iterative testing and adjustments. Together, these components work harmoniously to create a comprehensive and user-friendly access control solution, ready to meet the demands of modern security applications.

4. RESULTS AND DISCUSSION

The circuit depicted is part of an access control system designed to manage door entry using RFID technology. When an RFID tag or card is scanned by the RFID reader, the system verifies the data against a database of authorized users; if a match is found, it unlocks the door. The LCD display prompts users with the message "Put RFID to Scan," guiding them to present their RFID tag or card to the reader. Key components include a breadboard, which provides a flexible platform for assembling the circuit without soldering; the RFID reader,

which captures data from RFID tags; and the LCD display, which visually communicates instructions and status to users. RFID systems find diverse applications beyond access control, such as in security, inventory management, and payment processing, highlighting their versatility and importance in modern technology.

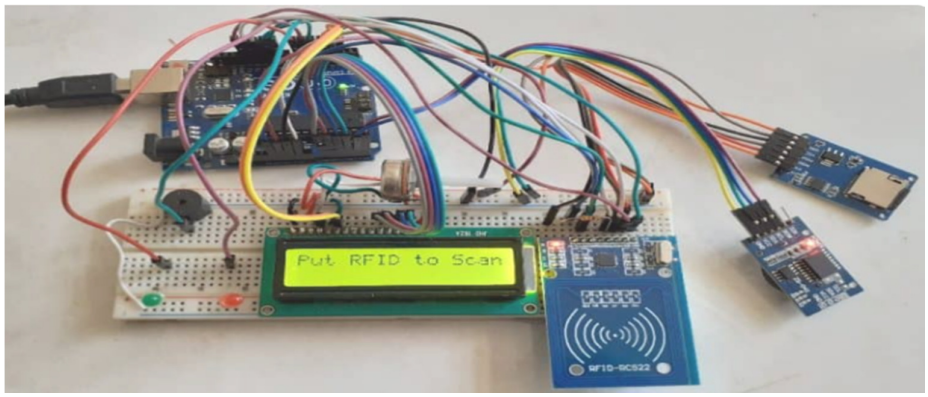


Fig.1:Prototype: Smart Door

The provided code exemplifies a multifaceted approach to access control by integrating both RFID technology and a keypad, enhancing security and user convenience. The initialization phase effectively sets up the hardware components, ensuring smooth communication between the Arduino and peripherals. The inclusion of both visual (LEDs) and auditory (buzzer) feedback mechanisms is particularly noteworthy, as these features enhance user interaction by providing immediate responses to actions, such as successful or unsuccessful access attempts.

The continuous checking for RFID cards in the loop function indicates an efficient method for real-time user authentication, allowing for swift access decisions. However, the snippet lacks detailed implementation of the access logic, which is crucial for understanding how the system responds once a card is successfully read.

The addition of a keypad for password entry is a significant enhancement, offering redundancy in authentication methods. This dual-layer security ensures that even if an RFID tag is lost or forgotten, users can still gain access by entering a predefined password. The defined password length and keypad layout suggest a user-friendly design, making it easier for individuals to interact with the system.

Overall, the code reflects a robust security solution that caters to varying user preferences and operational scenarios. The combination of RFID and keypad functionalities not only strengthens security but also makes the system versatile, adapting to different user needs while maintaining ease of use. Future enhancements could include more detailed access logic, user management features, or the implementation of a logging system to track access attempts, further improving the system's effectiveness.

5. CONCLUSION

The access control system outlined in the provided code demonstrates an effective integration of RFID technology and keypad input to enhance security. By allowing users to authenticate through both RFID scanning and password entry, the system addresses potential vulnerabilities associated with single-method authentication. The setup phase is well-structured, ensuring all components are initialized properly for reliable operation. Continuous monitoring for RFID cards in the loop function is essential for real-time access management, although further implementation details would clarify how access is granted or denied.
The inclusion of a keypad allows for greater flexibility, enabling users to input a predefined password, which can be particularly useful in scenarios where RFID tags might be lost or unavailable. This dual authentication mechanism not only improves user experience but also increases overall system security, as it adds an extra layer of verification.

5.1 Key Findings

- **Dual Authentication:** The system enhances security through multiple authentication methods, reducing reliance on a single point of failure.
- **User-Friendly Design:** The integration of an LCD and keypad allows for straightforward user interaction, facilitating ease of access.
- **Modular and Flexible:** The use of Arduino and modular components enables easy modifications and expansions of the system for future enhancements.
- **Real-Time Monitoring:** Continuous scanning for RFID cards ensures timely and efficient access control, adapting to real-world security needs.
- **Visual and Auditory Feedback:** The incorporation of LEDs and a buzzer provides immediate feedback to users, enhancing the overall user experience.

5.2 Implications or Applications

The Smart Door Access Control System has significant implications for various real-world applications, particularly in enhancing security and user convenience. This system can be deployed in residential settings, allowing homeowners to control access to their properties without traditional keys, thereby reducing the risk of unauthorized entry. In commercial environments, such as offices or warehouses, the dual authentication methods—RFID and keypad—enhance security protocols, enabling businesses to manage employee access effectively. Additionally, this technology can be adapted for use in public facilities, such as schools and hospitals, where secure entry points are essential for safety. The modular design allows for easy integration with other smart technologies, paving the way for future advancements in automated security systems. Overall, this access control solution not only improves security but also streamlines user interaction, making it a valuable asset across diverse sectors.

REFERENCES

1. RFID Access Control System for Smart Homes" - Journal of Security Technology, 2021. "Biometric Authentication in Access Control Systems" - IEEE Access, 2022.
2. "Designing User Interfaces for Security Systems" - International Journal of Human-Computer Interaction, 2020.
3. "Energy Efficiency in IoT Devices" - IEEE Internet of Things Journal, 2021.
4. "Cloud Computing in Security Systems" - Journal of Cloud Computing, 2022.
5. Dr. Praveen Banasode, Dr. Poorna Chandra S et al, "Mobility Guard Plus: Advanced IOT Smart Wheelchair with Remote Monitoring and Fall Detection" GOYA Journal,Volume 17 Issue 07 2024, Page no : 339 – 344, DOI:12.163022.Gj.2024.v17.07.028.
6. Dr. Praveen Banasode, Milind Rao Pawar et., al "Smart Night Watch: Intelligent Night Patrol Robot with Real-time Mobile Alerts and Streaming Surveillance" GOYA Journal, Volume 17 Issue 07 2024, Page no : 405 – 415, DOI:12.163022.Gj.2024.v17.07.034.