ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2773-6202 (Online)
CODEN: JTIOCC

Journal of Technology & Innovation (JTIN)

DOI: http://doi.org/10.26480/jtin.01.2026.54.57

REVIEW ARTICLE

CONSTRUCTION OF A CONTACTLESS KEY CARD ACCESS CONTROL SYSTEM USING A RADIO FREQUENCY IDENTIFICATION (RFID) SCANNER AND ARDUINO

Ojo Kennedy Odu*

Department of Science Laboratory Technology, University of Benin, Benin City, Nigeria
****Corresponding Author Email: kennedy.ojo@uniben.edu***

ARTICLE DETAILS

Article History:

Received 23 February 2026
Revised 25 March 2026
Accepted 29 April 2026
Available online 25 May 2026

ABSTRACT

Security is needed more and becoming more important in today's world. Sometimes, physical security and access control is not always the best solution, especially in instances with large crowd or systems that requires round-the-clock security. For this reason, an Arduino-based access control system using RFID (Radio Frequency Identification Technology) was created to provide security and access control to buildings and physical spaces, and this eliminated the need for physical security at all times. The device makes use of RFID technology and Arduino to complete its work. RFID (Radio Frequency Identification) is a communication technology commonly known as electronic tags. Radio transmissions can identify targets and transfer data without direct communication. Advancements in radio frequency recognition technology have led to its widespread usage in identity documents, defense, and industrial control. When the RFID scanner recognizes a tag, it checks its UID to the stored database to ensure accuracy. Access is granted if the captured user's UID matches a previously saved UID; otherwise, access is denied.

KEYWORDS

microcontroller, radio frequency identification, key card

1. INTRODUCTION

In the contemporary landscape of facility management, the primary challenge remains the robust regulation of personnel within sensitive physical environments. Traditional security measures, such as mechanical locks or stationary personnel, often fail to provide the scalability and round-the-clock reliability required by modern institutions. Consequently, implementing digital access control has become a fundamental necessity to restrict physical entry to critical infrastructures effectively. These systems act as digital gatekeepers, enhancing safety by maintaining a precise log of entry and exit events, thereby ensuring the privacy and integrity of organizational assets (Dhanalakshmi et al., 2021; Simukali, 2019).

The transition toward contactless technology has revolutionized this domain. By utilizing Radio Frequency Identification (RFID) for authentication, organizations can bypass the logistical hurdles of physical keys and the human error inherent in manual security. Current trends in smart building technology emphasize the use of RFID-based smart doors, which offer a seamless balance between high security and user convenience (Khabarlak and Koriashkina, 2021). Furthermore, recent comparative analyses of modern authentication methods suggest that RFID remains superior to other contactless approaches in institutional settings due to its durability and cost-effectiveness (Zhao and Liu, 2023). Beyond security, the shift toward contactless models has been accelerated by global health requirements, emphasizing systems that minimize physical touch to prevent the spread of pathogens (Jiang et al., 2023).

At the core of this project is the synergy between the RFID scanner which serves as the primary authorization interface and the Arduino microcontroller, which functions as the decision-making hub. As demonstrated in contemporary security literature, these microcontroller-centric architectures provide a robust foundation for building scalable and customizable security hardware (Williams, 2022). Arduino's versatility allows it to process complex input data and execute various outputs, such as triggering solenoids or visual alerts (Simukali, 2019). By comparing a user's Unique Identifier (UID) against a pre-registered database, the system provides an unmanned, efficient, and highly reliable method for managing institutional access.

1.1 Radio Frequency Identification (Rfid)

RFID technology is a cornerstone of modern wireless communication, finding applications across diverse sectors including logistics, automated library management, and supply chain tracking (Nedelkovski, 2017). Early academic explorations into this field demonstrated the feasibility of RFID-based access control for university hostels, laying the groundwork for more sophisticated biometric integrations (Umar et al., 2014). Modern literature has expanded on these foundations by examining the security protocols governing RFID tags. For instance, recent studies highlight the importance of anti-collision algorithms and encryption to prevent "tag cloning," which remains a threat in standard passive RFID systems (Hassan and Khan, 2022). In addition to security, the efficiency of the MFRC522 reader, a common component in Arduino projects has been validated for its low power consumption and high reliability in short-range detection (Prasad et al., 2024). Furthermore, the integration of Internet of Things (IoT) capabilities with RFID systems has allowed for real-time data logging and remote notifications, as seen in systems utilizing Telegram bot APIs for instant alerts (Ahmad et al., 2020; JAIEA, 2025). This shift enables administrators to monitor access points remotely, providing a significant advantage in large-scale industrial applications. By combining multiple verification layers, such as RFID with PIN technology, developers can create hybrid authentication systems that significantly reduce the likelihood of identity theft. These advancements ensure that the system remains adaptable to both residential and high-security industrial requirements.

2. MATERIALS AND METHODOLOGY

2.1 Materials for Construction

To guarantee that the system functions properly, the appropriate

Quick Response Code	Access this article online	
	Website: www.jtin.com.my	**DOI:** 10.26480/jtin.01.2026.54.57

components for the access control system must be chosen. The key components used in this project are as follows:

- Transformer
- Diodes
- Capacitors
- Resistors
- Arduino Microcontroller (Arduino MC)
- Light Emitting Diodes (LEDs)
- Wires
- Voltage Regulators
- Transistors
- Liquid Crystal Display (LCD) and I2C Module
- RFID scanner
- RFID card
- RFID tag
- Solenoid locker
- Buzzer

The selection of hardware components is critical to the longevity and precision of an access control system. The following materials were selected based on their technical specifications and compatibility with the Arduino ecosystem:

- **Arduino Uno Microcontroller:** Chosen for its robust processing capabilities and extensive library support for SPI and I2C protocols. Microcontrollers are significant for their capacity to efficiently manage the operation of electronic devices, facilitating automated processes across various applications.
- **RFID-RC522 Module:** A high-integration transmission module for contactless communication at 13.56 MHz (Prasad et al., 2024). It is valued for its ability to transmit user identities with minimal human intervention.
- **Solenoid Bolt Lock:** Provides the physical locking mechanism, requiring a 9V-12V pulse to actuate.
- **I2C Liquid Crystal Display (LCD):** Used to reduce the number of required pins on the Arduino while providing real-time feedback to the user.
- **Power Management Components:** Including L7805 voltage regulators to ensure a steady 5V supply to the logic circuits, preventing thermal instability (Kumar and Singh, 2025). The strategic use of these widely available, low-cost components ensures the system is economically viable for mass deployment without sacrificing operational integrity (Verma and Agrawal, 2021).
- **Peripheral Alerts:** Visual (LEDs) and audible (Buzzer) indicators provide immediate status updates for granted or denied access events.

The system's modular design increases development efficiency and enables the easy deployment of new features or the future integration of secondary sensors (Babiuch and Foltynek, 2024). In specialized scenarios, such as vehicle rental or high-security zones, the Arduino can also be interfaced with GSM modules for dual-layer security through One Time Passwords (OTP).

2.2 Block Diagram of Proposed Design

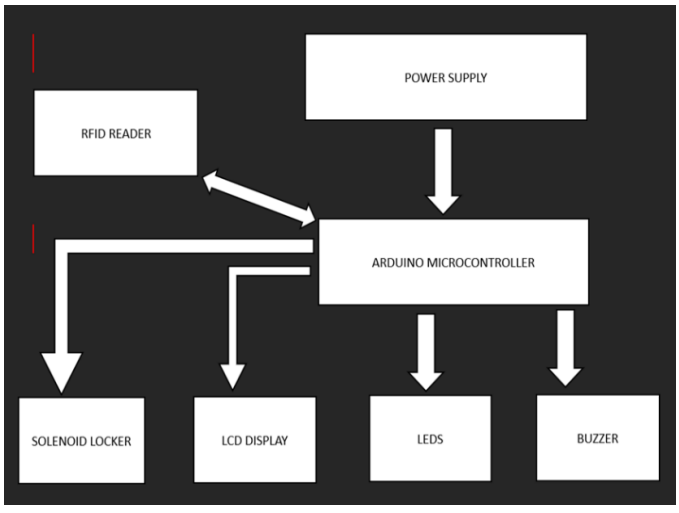


Figure 1: System Block Diagram

2.3 Mode of Operation

All the available Power or AC source are used as input into the power supply to make sure that as long as there is a supply from any of the AC sources, the system can be turned ON. The RFID reader is connected to the microcontroller and communication happens between them. Other components like the solenoid locker, buzzer, LEDs and LCD are connected to different pins in the microcontroller.

When the RFID reader scans a card or tag it gets the UID of the card or tag and sends it to the microcontroller as input. The code in the microcontroller runs and check if the UID is registered. If it is registered, the microcontroller gives an ouput to the green LED, the LCD, the buzzer and the solenoid locker for some seconds. If the UID is not registered, the microcontroller gives an output to the red LED, and the LCD for some seconds.

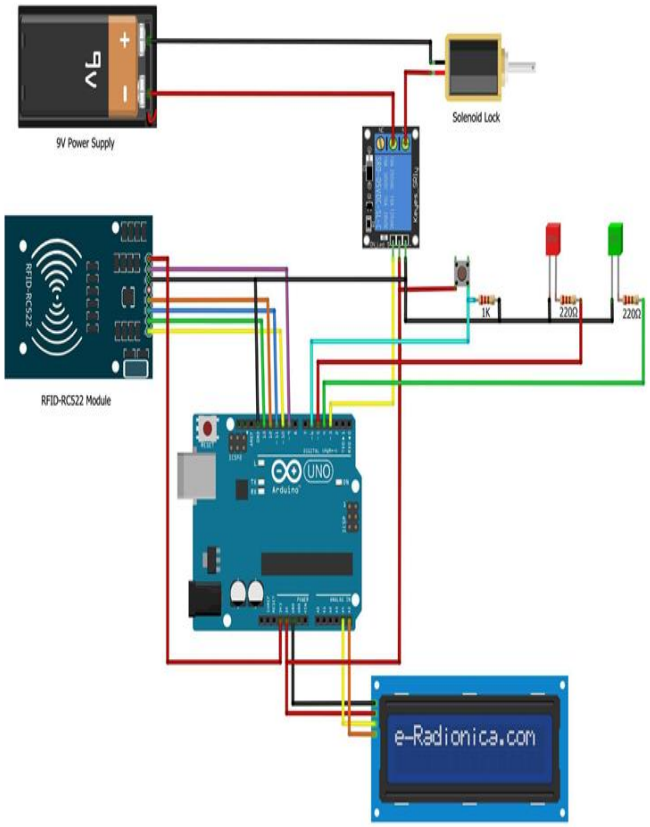


Figure 2: Complete Circuit Diagram

3. RESULT

3.1 System Testing

After the model is completed, testing is required to confirm that the system performs properly per the project's goals. The model has many components and circuitry that must be tested individually and collectively to ensure that the components work effectively, the individual circuits accomplish the function for which they were built, and the complete system functions well.

3.2 Test Plan

The test plan encompasses all the steps taken in checking the functionality of each module that makes up the entire system design.

3.3 Simulation

The test plan begins with a simulation of the complex work using an electronics software called Proteus. The simulation test results ensured that the system design was feasible and fully functional in its logical decision.

3.4 Power Supply Test

The setup for the power supply test circuit is shown in Figure 3 below. The setup comprises a 240V – 24V step-down centre tap transformer, a full wave rectifier, a 1000uf 100v filtering capacitor, and 1 voltage regulator (L7805CV). This test was carried out with no load connected.

Table 1: Power Supply Test	
Ac Input	**5 Volts Output**
212.35 V	5.04 V
215.57 V	5.08 V
204.17 V	5.06 V
195.19 V	4.99 V
188.20 V	4.97 V

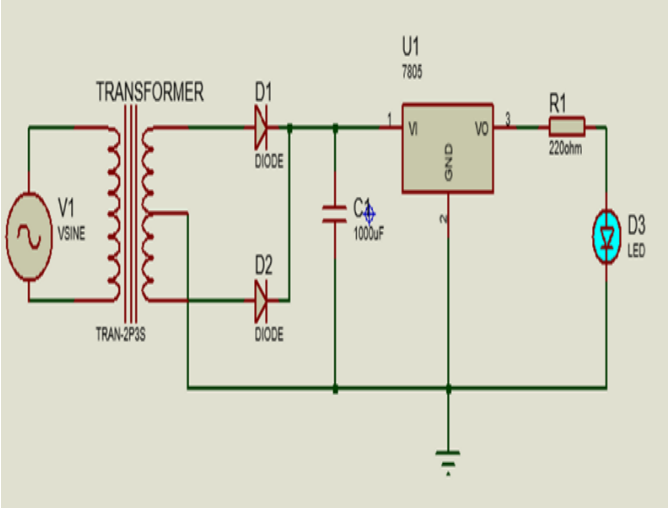
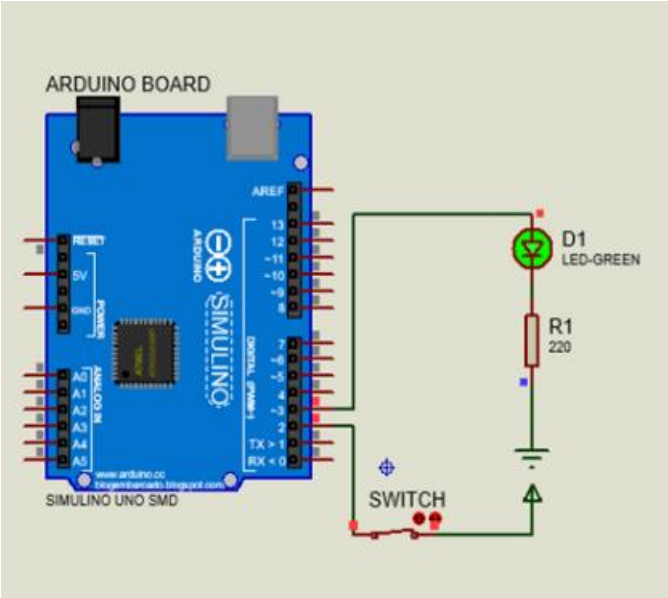


Figure 3: Power supply setup

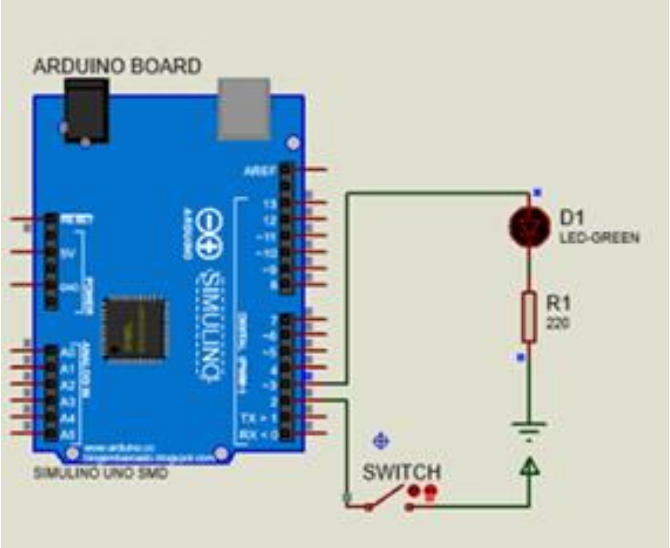
Table 1 shows a negligible voltage drop in the output of the voltage regulator. This is because the input AC voltage dropped. From the table above it can be deduced that the power supply design will still work fine. Even if the AC voltage input drops significantly to around 160V from the 240V expected, the voltage drop at the voltage regulators will not significantly affect the system.

3.5 Arduino Microcontroller And Led Circuit Test

The Arduino microcontroller is a crucial component in the system, as it receives input from the RFID reader and translates it into commands. The setup for the Arduino microcontroller and LED test circuit is shown in Figure 4.2 below. The setup comprises an Arduino Microcontroller Digital board, a 220ohm resistor, a switch or button and an LED. This test confirms that the Arduino Board and the Arduino Software are all working properly.



(a) Setup with open switch



(b) Setup with closed switch

Figure 4: Arduino Microcontroller and LED setup

From Figure 4 above, when the switch is open as in Figure (a), the LED is off, and when the switch is closed as in Figure (b), the LED turns on. This test confirms that both the Arduino board and the Arduino software are working as expected.

The code to test the LED with the Arduino microcontroller can be found in Appendix A.

The typical maximum current the LED can work with is roughly 25mA, and the Arduino board gives an output of 5V. This means the total resistance of the resistor we need to add and the LED should be:

$$R = \quad (1)$$

$$V = 5V, I = 25mA \simeq 0.025A \quad (2)$$

$$\therefore R = 5 / 0.025 \quad (3)$$

$$R = 200\Omega \quad (4)$$

The resistance of the LED would be extremely small in this direction, thus the resistance of the resistor would be larger than 200 Ohm. For safety reasons, we used 220 Ohm which still worked.

3.6 LCD With I2c Module Circuit

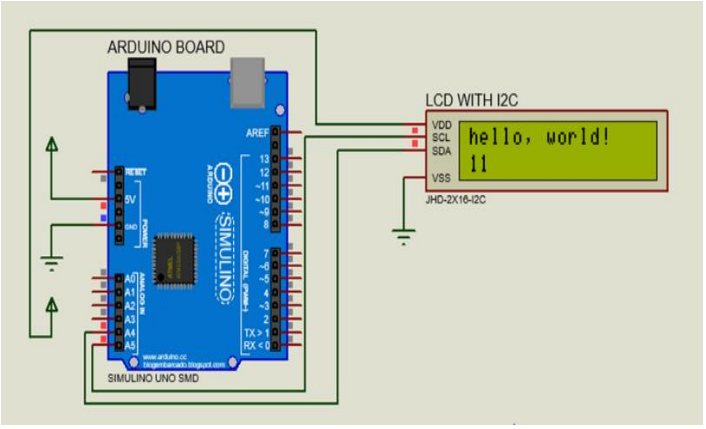


Figure 5: Arduino Microcontroller and LCD with I2C module setup

Figure 5 above shows the setup for the LCD to microcontroller circuit using the I2C module, simulated in the Proteus CAD software. The setup above consists of an Arduino microcontroller and a 2 by 16 Liquid Display Crystal (LCD).

The code to test the LCD to microcontroller circuit using the I2C module can be found in Appendix B.

3.7 Complete Access Control System Circuit Test

After the setup was completed, a full system test was carried out using an RFID card and an RFID tag. This test was carried out to verify the

connectivity of the system as well as to make sure the code and software were running properly. Figure 6 above shows the setup for testing the circuit simulated using the Proteus CAD software. This set consists of an Arduino microcontroller, two LEDs, three resistors, a capacitor, an LCD, a solenoid lock, a buzzer, an RFID reader, a 9v battery, and 5v power terminal from the power supply. The code in Appendix C was uploaded into the microcontroller to control the access based on the UID of either an RFID card or tag and these controlled the turning ON and OFF of the LED circuit. A prompt, a success message and an error message were displayed on the LCD based on whether access is gained or not, and the buzzer makes a sound if access is gained. The system was tested with an RFID card with a UID that was allowed access by the controller code and an RFID tag with an unknown UID. When both were scanned by the RFID reader, the card was successfully granted access while the tag wasn't granted access.

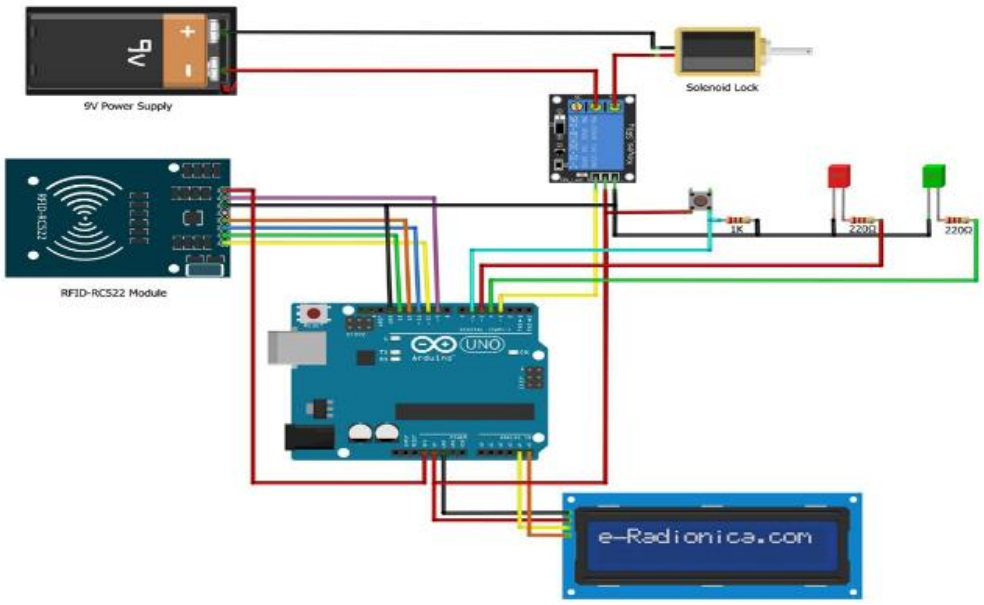


Figure 6: Complete access control system setup

4. Discussion

After considering the physical design of the hardware, as well as the installation of the components, the RFID and Arduino-based access control system was successfully developed and implemented. The system was able to grant access to an RFID card with known and registered UID and rejected access to an RFID tag with unknown UID.

5. Conclusion

The design and construction of an RFID and Arduino-based access control system offers numerous benefits for efficient and effective security and access control management. The developed system is also flexible in a way that each RFID card and RFID tag can be registered and unregistered in the system using the microcontroller code. The system can be widely applied to both personal and industrial systems, and it can easily be modified to include more security measures. With this system, security need not be physical and this can be extremely advantageous especially with systems and spaces that requires security at all times.

References

Ahmad, S., Al-Qerem, A., and Al-Zubi, M., 2020. IoT-based security systems: A review of RFID and sensor integration. International Journal of Advanced Computer Science and Applications, 11 (4), 112-119.

Babiuch, M., and Foltynek, P. 2024. Benefits of using design patterns on microcontrollers in implemented IoT applications. Sensors, 24 (23), 7803. https://doi.org/10.3390/s24237803 Cited by: 1

Design of door security system using Rfid based on IoT at Stmik Kaputama. 2025. JAIEA. https://ioinformatic.org/index.php/JAIEA/article/download/1367/990

Dhanalakshmi, K.S., Praghna, A., Reddy, E.T., and Prabhavathy, S.K. 2021. RFID based access control system using Arduino. Annals of the Romanian Society for Cell Biology, 25 (6), 17614-17622.

Hassan, M., and Khan, A. 2022. Security analysis of passive RFID systems in smart environments. Journal of Cyber Security and Mobility, 11 (2), 245-268.

Jiang, Y., Lai, P.L., Yang, C.C., and Wang, X. 2023. Exploring the factors that drive consumers to use contactless delivery services in the context of the continued COVID-19 pandemic. Journal of Retailing and Consumer Services, 72, 103276. https://doi.org/10.1016/j.jretconser.2023.103276 Cited by: 81

Khabarlak, K., and Koriashkina, L. 2021. Mobile access control system based on RFID tags and facial information. arXiv:2105.04874 [cs.CR].

Kumar, R., and Singh, P. 2025. Power optimization in microcontroller-based security hardware. Journal of Electronics and Electrical Engineering, 14 (1), 88-102.

Nedelkovski, D., 2017. How RFID works and how to make an Arduino-based RFID door lock. HowToMechatronics.

Prasad, V., Reddy, S., and Gupta, N. 2024. Technical evaluation of MFRC522 modules for institutional attendance tracking. Sensors and Actuators: A Physical, 368, 115-127.

Simukali, C. M. 2019. Multi factor authentication access control for student and staff based on RFID, barcode and GIS (Doctoral dissertation, University of Zambia).

Umar, F., Hasan, M., Amar, M., Hanif, A., and Asad, M. U. 2014. RFID based security and access control system. IACSIT International Journal of Engineering and Technology, 6 (4), 309-314.

Verma, S., and Agrawal, R. 2021. Implementation of Arduino-based low-cost security systems. Journal of Embedded Systems and Applications, 9 (3), 12-24.

Williams, J. 2022. Advanced Microcontroller Projects for Security. Academic Press.

Zhao, H., and Liu, Y. 2023. Comparative study of contactless communication technologies for access control. Applied Sciences, **13** (4), 2101.