Journal of Computer Science and Technology
Volume 4 ; Number 3 ; September 2026 ; Page 125-133
DOI : https://doi.org/10.59435/jocstec.v4i3.793
https://jurnal.padangtekno.com/index.php/jocstec
E-ISSN : 2985-4318
P-ISSN : 2985-5772

Development Of A Non-Intrusive RFID Elevator Access Control System For Residential Buildings

Parade Parsaulian Purba[1], Vivin Octowinandi[2], Prasaja Wikanta[3], Muhammad Arifin[4]

[1234] Jurusan Teknik Elektro, Prodi Teknik Elektronika Manufaktur, Politeknik Negeri Batam, Indonesia
antok@polibatam.ac.id

ABSTRACT

This study developed and evaluated a standalone, non-intrusive radio frequency identification (RFID)-based elevator access control system for a four-story residential building. The system used an Arduino Uno, an MFRC522 RFID reader, and relay interfaces to regulate access to Floors 2, 3, and 4. Authorized card identifiers and floor permissions were stored locally, enabling offline operation without an external database or network connection. The relays interfaced only with the elevator push-button circuits and did not modify the original controller, motor drive, door mechanism, or safety system. Performance was evaluated using 47 registered cards and three unregistered cards, with each card tested 50 times, producing 2,500 authentication trials. Under the tested conditions, all registered cards were correctly authenticated according to their assigned floor permissions, while all unregistered cards were rejected. The system achieved 100% authentication accuracy, 100% correct relay activation, and 100% unauthorized-card rejection. Stable card detection was obtained at distances of up to approximately 1 cm. The first-floor button remained independent of the RFID module to preserve minimum accessibility during module failure. The proposed system provides a practical and low-cost retrofit solution for floor-specific elevator access control in small residential buildings.

Keyword: RFID; elevator access control; Arduino Uno; relay interface; access authorization; standalone system

INTRODUCTION

Radio frequency identification (RFID) has been widely applied in access control systems because it enables rapid and contactless user identification through unique data stored in RFID tags. Compared with mechanical keys and password-based systems, RFID offers simpler operation and more flexible authorization management, supporting its application in buildings, parking facilities, attendance systems, and restricted areas [1].

In multi-story residential buildings, elevators function not only as vertical transportation systems but also as access points to private residential floors. However, elevators in small apartments, boarding houses, and similar properties commonly allow users to select any destination floor without authorization. This condition may permit tenants, visitors, or unauthorized individuals to enter floors beyond their permitted areas, thereby reducing resident privacy and increasing the risk of unauthorized access.

Previous studies have demonstrated the feasibility of RFID-based elevator authorization. Kishan *et al.* [2] developed an RFID-based system that assigned different elevator access permissions to registered users, while Desmira *et al.* [3] applied RFID authentication to improve elevator security in a campus building. RFID has also been integrated with programmable logic controllers (PLCs) and human–machine interfaces (HMIs) for elevator authorization and priority-based access control [4],

E-ISSN : 2985-4318
P-ISSN : 2985-5772

[5]. These studies demonstrate that RFID technology can provide reliable user identification and differentiated floor authorization.

Nevertheless, many existing systems require integration with proprietary elevator controllers, PLCs, external databases, or network-based management platforms. Such configurations may increase installation costs, technical complexity, maintenance requirements, and dependence on elevator manufacturers. Direct intervention in the original elevator controller may also create compatibility and safety concerns, particularly when an access-control system is added to an existing elevator.

A retrofit approach can provide additional functionality without replacing the primary elevator controller. Rubies *et al.* [6], for example, introduced a non-contact and non-intrusive add-on device for wireless elevator control. However, limited research has examined a standalone RFID retrofit system that restricts floor access exclusively through the elevator push-button circuits. In this architecture, the authorization module does not control elevator movement, doors, motor drives, braking, or safety functions. Instead, it temporarily enables the authorized push-button circuit, while the original elevator controller continues to execute all operational and safety processes.

Therefore, this study developed and evaluated a standalone, non-intrusive RFID-based elevator access control system for a four-story residential building. The system uses an Arduino Uno, an MFRC522 RFID reader, and relay interfaces to regulate access to Floors 2, 3, and 4. Card unique identifiers (UIDs) and floor-access permissions are stored locally in the embedded controller, eliminating the need for an internet connection, external server, or database. Following successful authentication, the corresponding relay enables the authorized floor button for approximately three seconds. The first-floor button remains independent of the RFID module to preserve minimum accessibility during power interruptions, maintenance, or controller failure.

The main contribution of this study is the implementation of a low-cost RFID authorization module that can be retrofitted to an existing elevator without modifying its original control and safety architecture. System performance was evaluated through 2,500 authentication trials involving 47 registered and three unregistered RFID cards. The evaluation focused on authentication accuracy, unauthorized-card rejection, floor-specific relay activation, standalone operation, and RFID reading distance.

METHOD

A. Research Design and System Architecture

This study employed an engineering design and experimental testing approach to develop and evaluate a non-intrusive RFID-based elevator access control system. The system was implemented on an operational four-story elevator at Green Kost, a residential boarding house. The development stages included requirement identification, hardware and firmware design, prototype assembly, installation, and functional testing.

The system was designed to meet four primary requirements: 1) standalone operation without an internet connection or external database; 2) installation without modifying the original elevator controller or safety system; 3) floor-specific authorization based on registered RFID cards; and 4) continued access to the first floor when the RFID module was inactive.

The system consisted of an Arduino Uno, an MFRC522 RFID reader, a four-channel relay module, an LM2596 voltage regulator, a buzzer, and a DC power supply. The Arduino Uno served as the main controller, while the MFRC522 reader operated at 13.56 MHz and communicated with the controller through the Serial Peripheral Interface (SPI) protocol [7], [8]. The reader supports proximity-card communication based on the ISO/IEC 14443 Type-A standard [9].

Authorized card unique identifiers (UIDs) and their corresponding floor-access permissions were stored locally in the Arduino program memory. Consequently, authentication was performed without network access, cloud services, or an external user database. The overall system architecture is presented in Fig. 1.

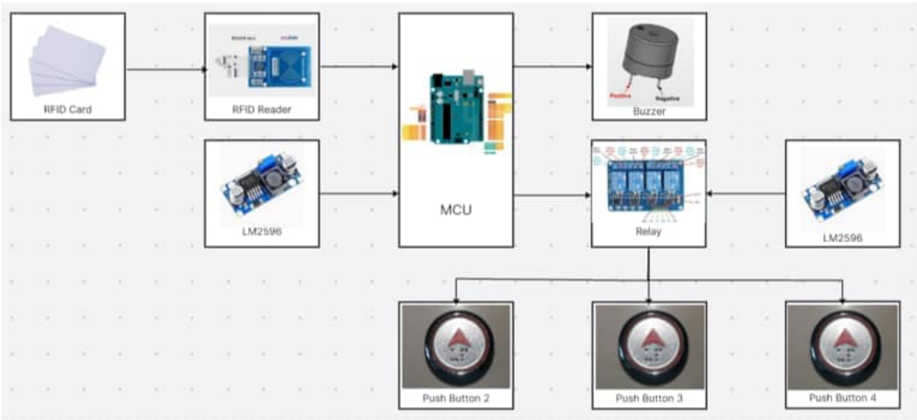

Figure 1. System block diagram

B. Hardware, Software, and Installation

The MFRC522 reader detected the UID of each RFID card, and the Arduino compared the detected UID with the registered credential list. When an authorized UID was recognized, the controller activated the relay associated with the assigned floor for approximately three seconds. During this interval, the user manually pressed the permitted elevator button. The relay then automatically returned to its inactive state, requiring a new authentication before another restricted floor could be selected.

Three relay channels were connected to the push-button circuits for Floors 2, 3, and 4, while the fourth channel was reserved for future expansion. Master cards were authorized for all three restricted floors, whereas floor-specific cards activated only the relay associated with their assigned floor. Unregistered cards did not activate any relay. The buzzer generated different audible signals for accepted and rejected authentication attempts.

The firmware was developed using the Arduino Integrated Development Environment (IDE) and performed RFID detection, UID comparison, access verification, relay selection, buzzer notification, timeout control, and return to standby mode. Embedded programming procedures followed established Arduino programming principles [10], [11].

The prototype was installed inside the elevator control panel. Relay contacts were connected in series with the destination-floor push-button circuits. When a relay was inactive, the corresponding restricted-floor button could not transmit an input to the elevator controller. Following successful authentication, the circuit was temporarily restored, allowing the original elevator controller to process the user's manual button input.

No connection was made to the elevator motor drive, door mechanism, braking system, emergency circuit, overload sensor, or other safety-related components. Therefore, the RFID module functioned only as an authorization interface. The first-floor push-button circuit remained independent of the module so that users could return to the primary exit floor during a power interruption, controller failure, or maintenance condition.

C. Experimental Testing

System performance was evaluated using 50 RFID cards, consisting of 47 registered cards and three unregistered cards. The registered cards comprised 11 master cards, 12 Floor 2 cards, 12 Floor 3 cards, and 12 Floor 4 cards. Each card was tested 50 times, producing a total of 2,500 authentication trials, as summarized in Table I.

Table 1. Experimental Testing Configuration

Card category	Number of cards	Tests per card	Total trials
Master card	11	50	550
Floor 2 card	12	50	600
Floor 3 card	12	50	600

Floor 4 card	12	50	600
Unregistered card	3	50	150
Total	**50**		**2,500**

A registered-card trial was classified as successful when the card was recognized and only the relay or relays permitted by its authorization level were activated. A master-card trial was considered successful when access to Floors 2, 3, and 4 was enabled. A floor-specific trial was considered successful when only the relay corresponding to the assigned floor was activated. An unregistered-card trial was classified as a successful rejection when no relay was activated.

RFID reading distance was also evaluated by positioning a card at approximately 0, 1, 2, and 3 cm from the reader surface. The response was classified as *detected* when the card was consistently recognized, *unstable* when detection was intermittent, and *not detected* when no identifier was received. Card orientation, antenna modification, electromagnetic interference, and radio-frequency field strength were not independently examined.

D. Performance Analysis and Safety Scope

System performance was evaluated based on registered-card authentication accuracy, relay-activation accuracy, unregistered-card rejection rate, and effective RFID reading distance. Authentication accuracy was calculated by dividing the number of successful registered-card trials by the total number of registered-card trials and multiplying the result by 100%. The rejection rate was calculated by dividing the number of correctly rejected unregistered-card attempts by the total number of unregistered-card attempts and multiplying the result by 100%.

Relay activation was considered correct when the activated channel matched the authorization assigned to the card. Failure to activate the required relay, activation of an unauthorized floor, or simultaneous unintended relay activation was classified as an unsuccessful trial. The results were analyzed descriptively using frequencies, percentages, and observed operating conditions because the experiment was intended as functional prototype verification rather than inferential comparison.

In this study, the term *non-intrusive* refers to the installation approach in which the added module interfaces only with the destination-floor push-button circuits. The module does not control elevator movement, speed, braking, doors, emergency operation, or certified safety functions. Therefore, the independent first-floor access provides minimum accessibility during RFID module interruption but does not replace the elevator manufacturer's safety and evacuation mechanisms.

RESULT AND DISCUSSION

A. Result

The RFID-based access control system was successfully assembled and installed on an operational four-story elevator at Green Kost. The implemented module comprised an Arduino Uno, an MFRC522 RFID reader, a four-channel relay module, an LM2596 voltage regulator, a buzzer, and supporting electrical components. Three relay channels were connected to the push-button circuits for Floors 2, 3, and 4, while the remaining channel was reserved for future expansion. The first-floor push-button circuit remained independent of the RFID module. The installed system is shown in Figure 2.

Figure 2. Installed RFID elevator access control module

During operation, the buttons for Floors 2, 3, and 4 remained inactive until a registered RFID card was presented. Successful authentication activated the appropriate relay for approximately three seconds, allowing the user to press the authorized floor button. The relay then returned automatically to its inactive state, and a new RFID authentication was required for subsequent access. Functional verification confirmed that the RFID reader, controller, buzzer, relay module, and push-button interface operated according to the programmed sequence. The system also returned automatically to standby mode after each successful or rejected authentication attempt.

B. Authentication and Floor-Authorization Performance

The system was evaluated using 47 registered cards and three unregistered cards. Each card was tested 50 times, producing 2,500 authentication trials. The registered cards consisted of 11 master cards and 12 cards assigned to each of Floors 2, 3, and 4. The authentication and relay-activation results are summarized in Table 2.

Table 2. Authentication and Relay-Activation Results

Card category	Total trials	Expected authorization	Successful trials	Success rate
Master card	550	Floors 2, 3, and 4	550	100%
Floor 2 card	600	Floor 2 only	600	100%
Floor 3 card	600	Floor 3 only	600	100%
Floor 4 card	600	Floor 4 only	600	100%
Unregistered card	150	No access	150 rejected	100%
Total	**2,500**	-	**2,500**	**100%**

All 2,350 registered-card trials were successfully authenticated. Master cards enabled the relay channels associated with all three restricted floors, while floor-specific cards activated only the relay

E-ISSN : 2985-4318
P-ISSN : 2985-5772

corresponding to their assigned floor. No cross-floor or unintended simultaneous relay activation occurred. The registered-card authentication accuracy was calculated as:

$$\text{Authentication accuracy} = \frac{2,350}{2,350} \times 100\% = 100\%$$

All 150 authentication attempts involving unregistered cards were rejected, and none activated a relay. The rejection rate was therefore:

$$\text{Rejection rate} = \frac{150}{150} \times 100\% = 100\%$$

The buzzer also generated the expected audible response: a confirmation signal for registered cards and a warning signal for unregistered cards. During each successful authentication, the authorized relay remained active for approximately three seconds before returning automatically to its inactive state.

C. Reading Distance, Standalone Operation, and Fail-Safe Performance

RFID reading performance was evaluated at approximate card-to-reader distances of 0, 1, 2, and 3 cm. The results are presented in Table 3.

Table 3. RFID Reading-Distance and Operational Results

Performance indicator	Result
Detection at 0 cm	Stable
Detection at 1 cm	Stable
Detection at 2 cm	Intermittent
Detection at 3 cm	Not detected
Stable operating distance	Approximately 1 cm
Internet connection	Not required
External database	Not required
First-floor access during module interruption	Available

The card was consistently recognized at distances of 0 and 1 cm. Detection became intermittent at approximately 2 cm, while no identification was obtained at 3 cm. Thus, the effective stable reading distance was approximately 1 cm. Throughout the experiment, authentication and authorization were performed locally using RFID identifiers and access permissions stored in the Arduino program memory. The system operated without an internet connection, external server, or database.

The first-floor button remained operational without RFID authentication and continued to function when the added module was disconnected from its power supply. This configuration preserved minimum access to the primary exit floor while access to Floors 2, 3, and 4 remained subject to RFID authorization. Overall, the prototype completed all 2,500 authentication trials without incorrect relay activation. Under the tested conditions, it achieved 100% registered-card authentication accuracy, 100% floor-authorization accuracy, and 100% rejection of unregistered cards.

D. Discussion

The experimental results demonstrate that the proposed RFID-based system successfully implemented floor-specific elevator authorization under the tested conditions. All 2,350 registered-card trials activated the relay outputs corresponding to the programmed access permissions, while all 150 unregistered-card attempts were rejected. No unintended relay activation was observed during the 2,500 trials. These findings indicate that the UID comparison, authorization mapping, relay-control logic, and automatic timeout function operated consistently during repeated functional testing.

The results are consistent with previous studies demonstrating the effectiveness of RFID technology for elevator-access authorization. Kishan *et al.* [2] implemented differentiated elevator-access permissions using RFID credentials, while Desmira *et al.* [3] applied RFID authentication to restrict elevator use in a campus building. Aryaditama *et al.* [4] similarly integrated RFID with programmable logic control for elevator security. The present study extends these applications by implementing RFID authorization through a standalone retrofit module rather than through direct integration with the elevator's primary controller.

The principal contribution of the developed system is its non-intrusive interface. The relay module was connected only to the destination-floor push-button circuits and did not control elevator movement, doors, braking, motor drives, or emergency functions. After successful authentication, the relay temporarily restored continuity to the authorized button circuit, while the original elevator controller continued to process movement and safety operations. This separation reduces installation complexity and limits modifications to the existing elevator architecture. The approach is also consistent with the retrofit principle demonstrated by Rubies *et al.* [6], although the present system specifically focuses on local RFID authentication and floor-level authorization.

Standalone operation provides another practical advantage. Card identifiers and floor-access permissions were stored in the Arduino program memory, allowing authentication without internet connectivity, cloud services, or an external database. This configuration may be appropriate for boarding houses and small residential buildings where the number of users is relatively stable and dedicated information-technology infrastructure is unavailable. It also reduces dependence on network availability and minimizes additional operational requirements. However, locally programmed credentials make card registration, deletion, and permission updates less convenient because each modification currently requires firmware changes.

The approximately three-second relay activation interval was sufficient during the experiment to allow authenticated users to press the authorized floor button while preventing the circuit from remaining continuously enabled. Automatic relay deactivation ensured that each restricted-floor selection required a new authentication process. Nevertheless, the activation period may require adjustment for elderly users, persons with mobility limitations, or occupants carrying large items. Future implementations could therefore incorporate configurable activation intervals and visual indicators in addition to the existing audible notification.

Stable RFID detection was obtained at distances of up to approximately 1 cm. Although this range is relatively short, it is suitable for intentional authentication because users must deliberately position the card near the reader. In an elevator cabin, such a short operating range may also reduce unintended detection of RFID cards carried by nearby passengers. Detection performance may nevertheless be influenced by card orientation, reader placement, enclosure materials, electromagnetic interference, and differences among RFID tags. These factors were not independently examined in the present study and should therefore be evaluated in future experiments.

The independent first-floor button maintained minimum operational accessibility when the RFID module was disconnected or inactive. Users could consequently return to the primary exit floor without RFID authentication. This configuration reduces the operational impact of authorization-module failure; however, it should not be interpreted as an elevator safety or evacuation system. Emergency operation, door protection, braking, overload detection, and other certified safety functions remain under the control of the original elevator system and manufacturer.

The observed 100% success rate should be interpreted within the limitations of the experimental design. Testing was conducted on a single four-story residential elevator under controlled operating conditions and primarily evaluated functional consistency. The experiment did not assess long-term reliability, relay wear, voltage fluctuations, temperature and humidity effects, loose wiring, electromagnetic disturbances, or continuous operation over extended periods. Compatibility with elevators employing different button voltages, controller architectures, or communication systems must therefore be evaluated before broader implementation.

Security is another limitation because authentication relied on RFID card UIDs. UID-based verification is sufficient for basic residential access restriction but may be susceptible to card cloning or credential emulation. Higher-security applications should therefore consider cryptographically protected credentials, encrypted card sectors, or additional authentication factors. Future development should also incorporate dynamic credential management, access-event logging, improved electrical isolation, surge protection, and compliance with applicable elevator and building-safety requirements.

Overall, the findings demonstrate that floor-access authorization can be added to an existing elevator without transferring control of movement or safety functions to the RFID module. The proposed architecture provides a practical balance among low implementation cost, standalone operation, floor-specific authorization, and limited intervention in the original elevator system. This finding is consistent with Candra *et al.* [12], who demonstrated that an Arduino-based embedded system could integrate user authentication and security functions into a practical prototype. It is also supported by Darsani *et al.* [13], who showed that Arduino and relay-controlled actuators could perform automated control operations according to programmed commands. These studies reinforce the feasibility of relatively simple microcontroller architectures for low-cost security and automation applications. Nevertheless, wider deployment of the proposed system requires further evaluation of security, long-term reliability, compatibility, and regulatory compliance.

CONCLUSION

This study successfully developed and implemented a standalone, non-intrusive RFID-based access control system for a four-story residential elevator. The system restricted access to Floors 2, 3, and 4 by temporarily enabling the authorized push-button circuits without modifying the elevator's original controller, movement mechanism, door system, or safety functions.

Testing involving 47 registered cards and three unregistered cards produced 2,500 authentication trials. Under the tested conditions, the system achieved 100% registered-card authentication accuracy, 100% correct floor-relay activation, and 100% rejection of unregistered cards. Stable RFID detection was obtained at distances of up to approximately 1 cm, while local credential storage enabled operation without an internet connection or external database. The independent first-floor button also maintained minimum access when the RFID module was inactive.

These findings indicate that the proposed system provides a practical and low-cost retrofit solution for floor-specific access restriction in small residential buildings. Nevertheless, broader implementation requires further evaluation of long-term reliability, credential-cloning risks, dynamic card management, access logging, electrical protection, compatibility with different elevator systems, and compliance with applicable safety regulations.

REFERENCES

[1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, 3rd ed. Wiley, 2010, doi: 10.1002/9780470665121.

[2] S. R. Kishan, S. Hameed, J. Charan, and Y. Srikar, "RFID-based elevator access control system," in *Proc. 15th Int. Conf. Computing Communication and Networking Technologies (ICCCNT)*, 2024, doi: 10.1109/ICCCNT61001.2024.10724057.

[3] D. Desmira, M. A. Hamid, L. Noviawati, T. A. Munandar, M. Martias, and D. Aribowo, "Intelligent security system in a campus building using RFID to improve security for elevator users," *ELINVO (Electronics, Informatics, and Vocational Education)*, vol. 8, no. 1, pp. 1–7, 2023, doi: 10.21831/elinvo.v8i1.57848.

[4] R. A. Aryaditama, I. Halimi, and A. Kusuma Wardhany, "Perancangan RFID pada HMI Haiwell sebagai sistem kemananan plant elevator berbasis PLC," *Seminar Nasional Teknik Elektro*, vol. 10, no. 1, pp. 83–87, 2024. [Online]. Available: https://prosiding.pnj.ac.id/index.php/SNTE/article/view/2404

E-ISSN : 2985-4318
P-ISSN : 2985-5772

[5] M. Y. Coşkun and M. Karalı, “The realization of a control algorithm and its PLC-based program able to authorize four different ranks of priority to elevator users,” *International Journal of Applied Mathematics, Electronics and Computers*, vol. 4, Special Issue 1, pp. 416–420, 2016, doi: 10.18100/ijamec.282823.

[6] E. Rubies, R. Bitriá, E. Clotet, and J. Palacín, “Non-contact and non-intrusive add-on IoT device for wireless remote elevator control,” *Applied Sciences*, vol. 13, no. 6, Art. no. 3971, 2023, doi: 10.3390/app13063971.

[7] Arduino, “Arduino UNO Rev3,” 2026. [Online]. Available: https://docs.arduino.cc/hardware/uno-rev3. [Accessed: Jul. 17, 2026].

[8] NXP Semiconductors, “MFRC522: Standard performance MIFARE and NTAG frontend,” Rev. 3.9, Product Data Sheet, 2016. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

[9] International Organization for Standardization, “Cards and security devices for personal identification—Contactless proximity objects—Part 1: Physical characteristics,” ISO/IEC 14443-1:2018, 2018. [Online]. Available: https://www.iso.org/standard/73596.html

[10] M. Margolis, B. Jepson, and N. R. Weldin, *Arduino Cookbook*, 3rd ed. O’Reilly Media, 2020.

[11] S. Monk, *Programming Arduino: Getting Started with Sketches*, 3rd ed. McGraw Hill, 2023.

[12] M. W. Candra, F. Amaluddin, and A. A. Suryanto, “Sistem keamanan sepeda motor menggunakan fingerprint dan GPS tracking berbasis mikrokontroler Arduino ATMega2560,” *Curtina*, vol. 3, no. 1, pp. 30–39, 2022, doi: 10.55719/curtina.v3i1.442.

[13] N. Darsani, D. K. Basuki, F. Amaluddin, A. Wijayanti, and A. Rochmah, “Rancang bangun pemberian pakan otomatis dan pengaturan suhu untuk optimasi proses ternak ayam menggunakan Arduino berbasis IoT (Internet of Things),” *Curtina*, vol. 4, no. 1, pp. 23–32, 2023, doi: 10.55719/curtina.v4i1.824.