Implementation of RFID Authorization for Restricted Elevator Access at Green Kost

Final Project

By:
Parade Parsaulian Purba (3222311004)

Electronics Manufacturing Engineering Study Program
Electrical Engineering Department
Politeknik Negeri Batam
2026

Statement of Authenticity of Final Project

I, the undersigned, certify that the contents of part or all of my Final Project entitled: "Implementation of RFID Authorization for Restricted Elevator Access at Green Kost" is my own work, completed without the use of unauthorized materials, and does not contain work created by others that has been presented as my own. All references cited or referred to have been written in full in the bibliography. If it turns out that my statement is not true, I am willing to accept sanctions in accordance with applicable regulations.

Batam, 05 March 2026

Parade Parsaulian Purba
NIM: 322231100

Approval sheet

The Final Project is structured to fulfill one of the requirements for obtaining a degree
Bachelor of Associate Engineer (AMd.T.)
in
Batam State Polytechnic

By:
Parade Parsaulian Purba (3222311004)

Session date: 13 July 2026

Approved by:

Examiner I
Muhammad Arifin, S.Si., M.Si.
NIP: 116161

Supervisor I
Vivin Octowinandi
S.Tr.T., M.Sc
NIP: 120242

Examiner II
Prasaja Wikanta, ST., MT.
NIP: 103026

Implementation of RFID Authorization for Restricted Elevator Access at Green Kost

Abstract

Many residential buildings operate elevator systems without access control mechanisms that restrict users from selecting unauthorized floors. Such unrestricted access may lead to potential security and privacy issues for building occupants. This research presents the development of an RFID-based authorization system designed to regulate elevator access at Green Kost, a residential building consisting of four floors. The proposed system employs RFID cards as user identification devices, an MFRC522 module to read the card data, and an Arduino Uno microcontroller that performs the authentication process and controls elevator floor activation through a relay module. Each RFID card registered in the system is associated with specific floor permissions, ensuring that users are only able to reach floors for which they have authorization. In this implementation, access to floors 2, 3, and 4 requires RFID verification, while floor 1 remains freely accessible as part of a fail-safe operational design. Experimental evaluation indicates that the system operates consistently with an average authentication response time of approximately 0.5 seconds, demonstrating its capability to restrict unauthorized elevator access effectively

Keywords: RFID, Elevator Access Control, Arduino Uno, Authorization System

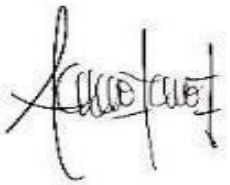
Foreword

Praise be to God Almighty for His blessings and grace, enabling the author to complete this journal entitled "Implementation of RFID Authorization for Restricted Elevator Access at Green Kost." This research was conducted as part of the final project in the Manufacturing Electronics Engineering Program at Batam State Polytechnic.

This paper presents the design, implementation, and evaluation of an RFID-based elevator authorization system developed to improve security by restricting access to designated floors according to user authorization. The proposed system integrates an MFRC522 RFID reader, Arduino Uno microcontroller, and relay-based control mechanism without modifying the original elevator operating system, making it suitable for practical implementation in residential buildings.

The author realizes that this journal is not free from limitations and therefore welcomes constructive suggestions for future improvement. It is hoped that this work can contribute to the development of RFID-based access control systems and serve as a useful reference for future research in building security and automation.

Batam, 05 March 2026



Parade Parsaulian Purba
NIM:32223110

Implementation of RFID Authorization for Restricted Elevator Access at Green Kost

Parade Parsaulian Purba1[1], Author2[1], and Author3[1*]

[1]Jurusan Teknik Elektro, Prodi Teknik Elektronika Manufaktur, Politeknik Negeri Batam, Batam, Indonesia

[*]Email: Parade.3222311004@students.polibatam.ac.id

Received on dd-mm-yyyy | Revised on dd-mm-yyyy | Accepted on dd-mm-yyyy

***Abstract*— Many residential buildings operate elevator systems without access control mechanisms that restrict users from selecting unauthorized floors. Such unrestricted access may lead to potential security and privacy issues for building occupants. This research presents the development of an RFID-based authorization system designed to regulate elevator access at Green Kost, a residential building consisting of four floors. The proposed system employs RFID cards as user identification devices, an MFRC522 module to read the card data, and an Arduino Uno microcontroller that performs the authentication process and controls elevator floor activation through a relay module. Each RFID card registered in the system is associated with specific floor permissions, ensuring that users are only able to reach floors for which they have authorization. In this implementation, access to floors 2, 3, and 4 requires RFID verification, while floor 1 remains freely accessible as part of a fail-safe operational design. Experimental evaluation indicates that the system operates consistently with an average authentication response time of approximately 0.5 seconds, demonstrating its capability to restrict unauthorized elevator access effectively.**

Keywords: RFID, Elevator Access Control, Arduino Uno, Authorization System

I . INTRODUCTION

Recent advances in security technology based on automatic identification have accelerated the adoption of modern access control systems. One widely used technology is Radio Frequency Identification (RFID), a wireless identification technology that enables authentication without direct physical contact. RFID offers convenience, speed, and a high level of reliability in the user identification process, making it widely used in security, attendance, parking, and room access control systems. In multi-story buildings equipped with elevators, access security is a critical aspect that requires attention. Unrestricted elevator use by all residents and visitors can lead to various issues, such as unauthorized access to restricted areas, reduced resident privacy, and increased building security risks. These issues are commonly found in vertical living spaces like apartments, dormitories, and multi-story boarding houses, which have numerous residents with varying access needs. Green Kost is a residential complex that uses elevators as a means of mobility between floors. In the current setup, any user can access all floor buttons without any access restriction mechanism. This situation poses a potential security risk because residents or guests may go to floors that are not their intended destination or to areas for which they do not have access permission. Therefore, a system is needed that can restrict elevator use based on the identity of registered users.[1]

A. Background

Advances in security technology based on automatic identification have driven the adoption of access systems that are more effective than conventional methods. The use of mechanical keys and manual access systems has various limitations, such as the risk of key loss, unauthorized access duplication, and the difficulty of monitoring users entering specific areas. Therefore, Radio Frequency Identification (RFID) technology is increasingly being implemented as a fast, contactless authentication solution capable of providing a unique identity for each user. [2]

RFID has been widely utilized in various security systems, such as building access control, inventory systems, smart home security, and the management of restricted areas requiring automatic user identification. This technology enhances identification accuracy and accelerates the verification process compared to conventional access methods. Additionally, RFID enables access restrictions based on predefined user rights, thereby reducing the potential for unauthorized use of facilities.[3]

In multi-story buildings equipped with elevators, safety is a key consideration. Elevators not only serve as a means of vertical transportation but also act as access routes to private areas or areas with specific security levels. Unrestricted elevator use can increase the risk of unauthorized individuals accessing certain floors, necessitating a control system capable of regulating user access based on their authorized privileges. Previous research indicates that integrating RFID into elevator systems can enhance user security by granting different access rights to each registered card.[1]

Green Kost is a multi-story residential building with different residents on each floor. Under current conditions, all residents can access all elevator floor buttons without any access restriction mechanism. This situation has the potential to cause privacy breaches, misuse of facilities, and a reduction in resident security. Therefore, a system is needed that can restrict elevator access based on the identity of registered users.

B. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is an automatic identification technology that uses radio waves to facilitate the recognition and exchange of data between a reader and an RFID tag. This technology enables identification without direct physical contact and does not require a line of sight, unlike barcode technology. Each RFID tag has a unique identity that can be used to distinguish one user from another, making RFID widely applied in security systems, inventory management, attendance systems, and building access control[2], [3].

Generally, an RFID system consists of three main components: the RFID tag, the RFID reader, and the data processing system. The RFID tag serves as a medium for storing user identity information; the RFID reader reads the data stored on the tag via radio frequency; while the data processing system performs verification and decision-making based on the information received from the reader[2]. In this study, the RFID reader used is the MFRC522 module, which is connected to an Arduino Uno via Serial Peripheral Interface (SPI) communication. Each RFID card has a Unique Identifier (UID) that serves as the user's identity to determine access rights to specific elevator floors.

RFID technology offers several advantages over conventional access methods, including fast authentication, ease of use, relatively low implementation costs, and the ability to flexibly manage user access rights. Additionally, RFID can enhance system security because only registered cards can gain access to protected facilities [4]. Research on RFID-based elevator access control systems also indicates that this technology can restrict elevator usage based on user authorization levels, thereby enhancing security and privacy in multi-story buildings [1]

In this study, RFID is used as the primary authentication method to control elevator access at Green Kost. When an RFID card is placed on the reader, the system reads the card's UID and compares it with the UID data stored on the Arduino Uno. If the UID is found in the list of registered users, the system activates the relay according to the user's access rights. Conversely, if the UID is not recognized, the system denies access and issues a notification via a buzzer. Through this mechanism, RFID serves as the primary component in the process of restricting elevator access based on user authorization levels.

C. Problem Statement

Despite the widespread use of elevators in multi-story residential buildings, many existing systems still operate without proper access control mechanisms. In such systems, users are able to freely select any floor without identity verification, which may lead to unauthorized access to restricted residential areas. This situation can potentially compromise the security and privacy of building occupants.

Based on these conditions, the problems addressed in this research can be formulated as follows:

1. How can an RFID-based authorization system be designed and integrated effectively with the elevator control system?
2. How can the system differentiate user access rights so that each RFID card can only activate the elevator for authorized floors?

D. Objectives

The main objective of this research is to develop an elevator access control system that utilizes RFID technology to regulate user access based on authorization levels. By implementing this system, elevator usage can be restricted so that users are only able to access floors that correspond to their assigned permissions.

The specific objectives of this study are as follows:

1. To design and develop an RFID-based authorization system that can be integrated with an elevator control system.
2. To implement a user access management mechanism in which each RFID card is assigned specific floor permissions.

E. Advantages

The implementation of an RFID-based elevator access control system provides several advantages in terms of security and operational efficiency. By integrating user identification with elevator access management, the system is able to regulate the use of elevator facilities more effectively.

First, the system improves building security by ensuring that only authorized users can access specific floors. Each registered RFID card contains a unique identification code that is linked to predefined access permissions. This mechanism helps prevent unauthorized individuals from entering restricted residential areas.

Second, the system enhances operational efficiency by automatically activating elevator floor buttons based on user authorization. This automated process reduces the possibility of improper elevator usage and allows floor access to be controlled systematically. As a result, the elevator system can operate in a more organized and secure manner within the Green Kost residential environment.

F. Components of the RFID Access Card System for Elevator Usage

The RFID-based elevator access control system consists of several hardware components that work together to perform user identification, authorization processing, and elevator control. These components are integrated to ensure that the authentication process operates reliably and that elevator access can be restricted according to the predefined permissions assigned to each RFID card. The system begins with the identification process using an RFID card, followed by data processing in the microcontroller, and finally the activation of the elevator floor button through an electronic switching mechanism.

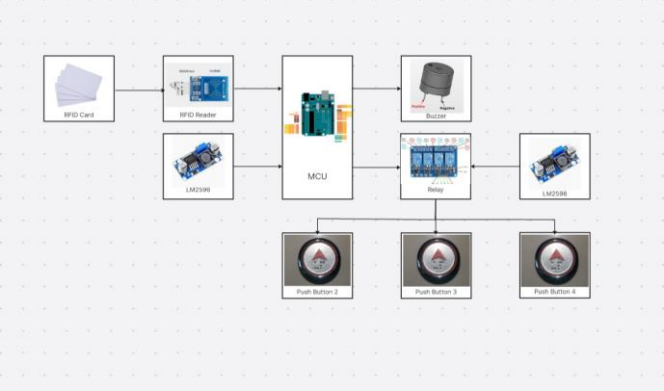
The main components used in the RFID elevator authorization system are described as follows:

1. RFID Card (Tag)
2. RFID Reader (MFRC522)
3. Microcontroller (Arduino Uno)
4. Relay Module
5. Power Supply Unit
6. Buzzer Indicator
7. LM2596

G. System Block Diagram

The system block diagram represents the overall architecture of the RFID-based elevator authorization system. The system begins with an RFID card that functions as the user identification medium. When the card is scanned by the RFID reader module, the reader retrieves the unique identification number stored in the card and sends the data to the microcontroller for processing. The microcontroller acts as the central control unit that compares the received UID with the list of registered UIDs stored in the Arduino program memory. If the UID matches one of the registered UIDs and the corresponding access permission is valid, the microcontroller activates the relay channel assigned to the authorized elevator floor. This mechanism allows the elevator to move only to floors that are authorized for that specific user.

Figure 1. System Block Diagram.

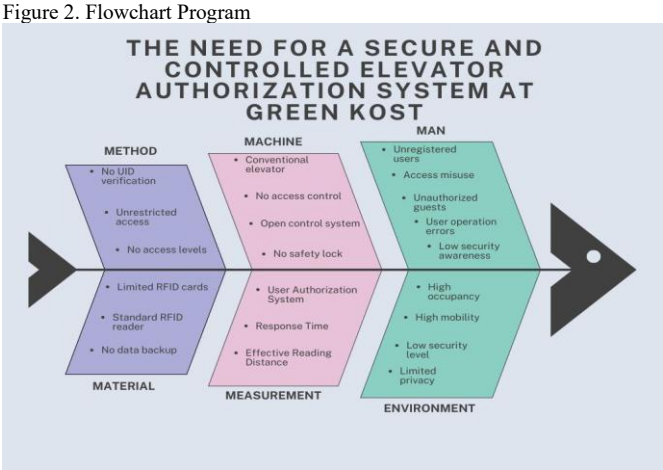


The overall interaction among the RFID reader, microcontroller, relay module, buzzer, and elevator control interface is illustrated in Figure 1.

H. Problems Analysis Using Fishbone Diagram

An analysis of the elevator access system problems at Green Kost was conducted using a fishbone diagram (cause-and-effect diagram) to identify the root causes affecting the level of security and access control. This approach was used to map the various contributing factors that led to the weak authorization system for conventional elevator use.

Figure 2. Flowchart Program



Through this structured analysis, several weaknesses related to user authorization, system control mechanisms, supporting components, and operational conditions were identified. The complete cause-and-effect relationship is presented in Figure 2.

The problems were analyzed based on six main aspects, namely Man (Human), Machine (Hardware), Method (Procedure), Material (Components), Measurement (Testing and Evaluation), and Environment. Each aspect represents interrelated sources of problems, such as the absence of user identity verification, elevator access without floor restrictions, an open control system, limitations in security support components, and low user awareness of access security.

I. Working principle of elevator buttons (NO/NC)

Elevator floor selection buttons generally operate based on the electrical switch principle using a Normally Open (NO) configuration. In the default condition, the circuit remains open and no electrical current flows through the system. When the button is pressed by the user, the contact closes and allows current to flow, sending a signal to the elevator control system to move to the selected floor.

In the proposed RFID authorization system, the manual button pressing process is replaced by a relay-controlled mechanism. After the RFID authentication process confirms that the user has valid access rights, the microcontroller activates the relay connected in parallel with the elevator button circuit. This action simulates the physical pressing of the button and triggers the elevator to move to the authorized floor. By implementing this method, floor access restrictions can be applied without modifying the internal control system of the elevator.

J. Comparison between commercial and proposed systems

To justify the implementation of the proposed RFID-based elevator authorization system, a comparison was conducted between commercially available elevator access control systems and the proposed solution. The comparison focuses on key engineering aspects, including implementation cost, installation requirements, and the level of modification required for the existing elevator system.

TABLE I
COMPARISON BETWEEN COMMERCIAL ELEVATOR ACCESS CONTROL SYSTEMS AND THE PROPOSED RFID-BASED SYSTEM

Aspect	Commercial System	Proposed RFID System
Initial Cost	Relatively high	Low-cost implementation
Installation	Requires vendor integration	Can be installed externally w modification
Elevator Modificati on	May require modification of the existing controller	No modification to the origin system

Table I shows a comparison between commercial elevator access control systems and the proposed RFID-based system. Compared with commercial solutions, the proposed system offers a more economical implementation, can be installed with minimal changes to the existing infrastructure, and does not require modification of the original elevator control system. These characteristics make the proposed system suitable for small-scale residential buildings such as Green Kost, where cost-effectiveness and ease of implementation are important considerations.

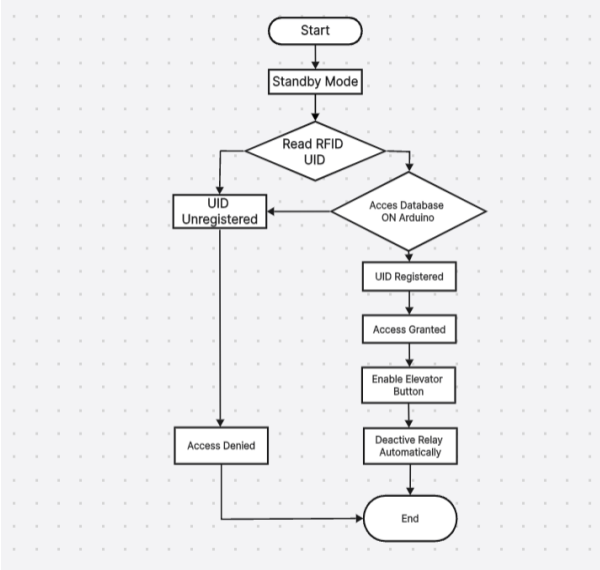
II . METHOD

This research applies an experimental approach to design and evaluate an RFID-based authorization system for elevator access control at Green Kost. The method focuses on the development of a hardware and software system that integrates RFID technology with a microcontroller to regulate elevator floor access based on user authorization. The overall process includes system design, hardware implementation, software development, and system performance testing. Through this method, the functionality and reliability of the proposed system can be analyzed under real operational conditions.

A. Flowchart Program

This flowchart illustrates that the system works by matching the RFID card's UID against a list of UIDs stored in the Arduino's memory. Registered cards are granted access to activate the relay and use the elevator, while unregistered cards are immediately denied access. This approach results in a simple, fast, and effective access control system that enhances elevator security.

Figure 3. Flowchart Program

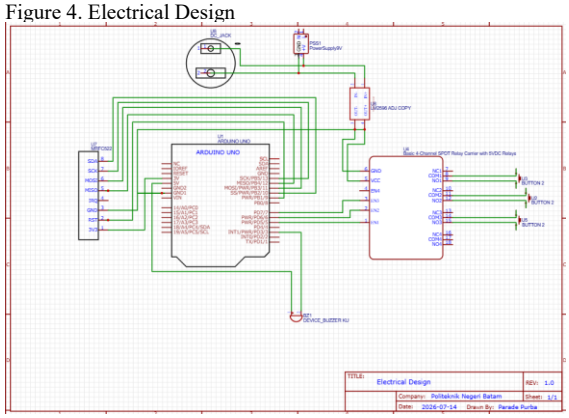


This sequence ensures that only registered users are able to activate the elevator floor corresponding to their assigned access rights. The detailed program flow is illustrated in Figure 3.

B. Electrical Design

This electrical design operates on the principle that an RFID reader reads the card's UID and sends it to the Arduino for verification. If the UID matches the list stored in the program's memory, the Arduino will activate the corresponding relay, allowing the elevator button to be used for a specific period of time. Once the access time expires, the relay will automatically turn off to deactivate the elevator button again. With this design, the system provides secure, simple, and easy-to-implement access control for elevator systems.

Figure 4. Electrical Design



The electrical design was developed to establish communication and control among all hardware components used in the system. The Arduino Uno functions as the central processing unit, receiving UID information from the RFID reader and controlling relay outputs according to the assigned access permissions. Additional components, including the buzzer and power regulation modules, support system operation and user notification functions. The interconnection of these components is presented in Figure 4.

C. Desain Mechanical

C.1 Controller Box Enclosure

An RFID Elevator Control Box cover offers several benefits, including protecting components, reducing the risk of short circuits caused by contact with foreign objects, and enhancing the overall aesthetics of the system.

Figure 5. MCU Cover

Figure 5 shows the controller box enclosure used to house the main control components of the RFID-based elevator authorization system. The enclosure provides physical protection for the Arduino Uno, relay module, power supply, and supporting circuitry against dust, accidental contact, and external disturbances during system operation.

C.2 RFID Reader Enclosure

The reader cover is designed separately from the MCU cover so that it can be installed in a location easily accessible to users, such as near the elevator control panel. The reader and the main control unit are connected via a socket cable, making installation more flexible and allowing maintenance to be performed without dismantling the entire system.

Figure 6. Reader Cover

Figure 6 shows the RFID reader enclosure used as the user identification interface in the proposed elevator authorization system. The enclosure houses the MFRC522 RFID reader module and provides a convenient location for users to present their RFID cards during the authentication process.

D. Tools

The development of the proposed RFID-based elevator authorization system requires several hardware devices and supporting equipment during the design, assembly, programming, and testing stages.

TABLE II
TOOLS USED IN THE DEVELOPMENT OF RFID-BASED ELEVATOR ACCESS CONTROL SYSTEM

No.	Tools	Specification	Quantity
1	Arduino Uno	ATmega328P microcontroller board	1 set
2	RFID Reader Module	RC522, 13.56 MHz	1
4	Relay Module	4 Channel, 5 VDC	1
5	Buzzer	Active Buzzer, 5 VDC	1
6	Transistor	BC547 NPN	1
7	DC-DC Step-Down Converter	LM2596 Adjustable Module	1
8	Reader Cover	-	1
9	Laptop	-	1
10	Digital Multimeter	Standard Digital Multimeter	1
11	DC Power Adapter	10-12 VDC, 3 A	1

Table II summarizes the tools used during the development of the RFID-based elevator authorization system. The listed equipment includes electronic development boards, measuring instruments, programming devices, and supporting hardware required for system assembly, testing, and verification. These tools facilitate the implementation process and ensure that each hardware component can be installed, configured, and evaluated properly.

E. Materials

The implementation of the proposed system also requires various electronic components and mechanical accessories to construct the hardware prototype.

TABLE III
MATERIALS USED IN THE DEVELOPMENT OF RFID-BASED ELEVATOR ACCESS CONTROL SYSTEM

No.	Materials	Quantity
1	RFID Card	49 Pcs
2	Prototype PCB	1 Pcs
3	Solder Wire	1 Roll
4	Header Pin	3 Set
5	Screw and Nut	12 Pcs
6	Spacer/Standoff	12 Pcs
7	Double-Sided Tape	1 Roll
8	Label Sticker	1 Sheet

Table III presents the materials used to assemble the RFID-based elevator authorization system. The listed materials consist of electronic modules, printed circuit board accessories, mechanical fasteners, and cable management components required to build a compact and reliable control unit. These materials support the integration of all hardware components into a functional prototype suitable for elevator access control applications.

F. Testing Objectives

Testing of this Radio Frequency Identification (RFID)-based elevator access authorization system prototype was conducted using a quantitative experimental approach with the following primary objectives:

1. Validating the User Authorization System Based on Access Levels (User Authorization System Validation)
   To test and ensure that the system can accurately distinguish user access rights on each elevator floor. This test verifies that the system correctly authenticates RFID cards by comparing their UIDs with the registered UID list stored in the Arduino program memory. Authorized cards activate the assigned relay, whereas unregistered cards are denied access (Access Denied).
2. Measuring System Authentication Response Time (Authentication Response Time Measurement)
   Measuring system processing speed performance by calculating the duration from when the RFID card is placed on the reader component until the microcontroller successfully processes the UID data and generates an action output (in the form of floor relay activation or access denial).
3. Determining the Effective Reading Distance of an RFID Antenna (Effective Reading Distance Determination)
   Identifying and establishing the maximum distance (in centimeters) between the RFID card and the MFRC522 reader module at which the reader module can still detect and read the card's data validly, stably, and consistently.
4. Testing System Success Rate and Operational Robustness (Success Rate and Robustness Testing)
   Assessing system reliability through the calculation of the success rate of card UID reads, rejection of foreign

cards, floor relay activation, and relay timeout functions. Additionally, this testing aims to measure the device's robustness against daily usage disruption scenarios, such as fast scanning, repeated scanning within short intervals, and scanning cards while they are inside the user's wallet.

III. RESULT

A. System Implementation Results

The elevator access control system was successfully implemented using an Arduino Uno as the main control unit, an MFRC522 RFID module as the card reader, a 4-channel relay as the actuator, and a buzzer as the audio indicator.

Figure 7. Electrical Desain

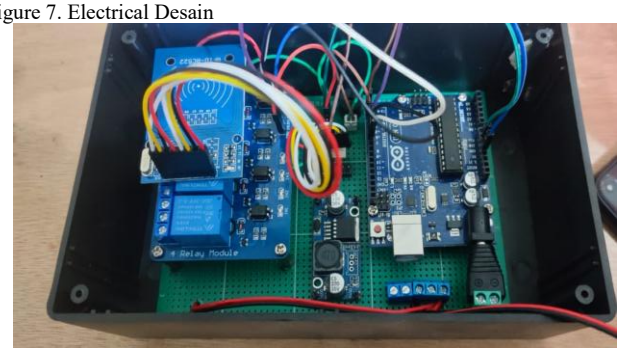


Figure 7 presents the assembled controller box of the proposed RFID-based elevator authorization system. The controller box integrates the Arduino Uno, MFRC522 RFID interface, relay module, DC-DC power converter, and supporting circuitry into a single enclosure, forming the main control unit responsible for user authentication and elevator access control.

B. Program Implementation Results & Relay Mapping

The software implementation was developed to manage user authorization based on the Unique Identifier (UID) stored in each RFID card. The program was written using the Arduino IDE and designed to perform card authentication, access validation, relay activation, and buzzer notification. When an RFID card is detected by the MFRC522 reader, the system reads the card UID and compares it with the list of registered UIDs stored in the microcontroller memory.

Each registered UID is assigned to a specific access category, namely Master Card, Relay 1 Card, Relay 2 Card, or Relay 3 Card. Based on the matching result, the Arduino Uno activates the corresponding relay associated with the authorized elevator floor. If the UID is not found in the registered database, the system rejects the access request and generates a warning indication through the buzzer. This approach allows the elevator access control process to be performed automatically without requiring manual floor authorization.

Figure 8. Mapping Program

```
#include <SPI.h>
#include <MFRC522.h>

// ================ RFID ================
#define SS_PIN 10
#define RST_PIN 9
MFRC522 rfid(SS_PIN, RST_PIN);

// ================ OUTPUT ================
#define BUZZER_PIN 3
#define RELAY1_PIN 5
#define RELAY2_PIN 6
#define RELAY3_PIN 7

// Relay active time (ms)
const unsigned long RELAY_ON_TIME = 3000;

// ======================================================
// MASTER CARD (11 UID pertama)
// ======================================================
const byte masterUIDs[11 ][4] = {
  {0xD3, 0x60, 0x0C, 0x2D},
  {0x53, 0x55, 0x14, 0x0D},
  {0x9A, 0xA0, 0x76, 0x06},
  {0x14, 0x9C, 0x74, 0x06},
  {0x2B, 0xC5, 0x75, 0x06},
  {0x1A, 0x6A, 0x73, 0x06},
  {0x81, 0x2C, 0xA5, 0x05},
  {0x87, 0x1F, 0x7A, 0x00},
  {0xF6, 0xFD, 0x74, 0x06},
  {0x6A, 0x1B, 0x74, 0x06},
  {0x87, 0x1B, 0x74, 0x06}
};
```

Figure 8 illustrates the program implementation used to map RFID card UIDs to their corresponding access categories and relay outputs.

Figure 9. Relay 1 Mapping

```
// Relay 1
const byte relay1UIDs[12][4] = {
  {0x8C, 0xFF, 0x74, 0x06},
  {0x1A, 0x5B, 0x77, 0x06},
  {0xFD, 0x56, 0x74, 0x06},
  {0x6C, 0xD6, 0x73, 0x06},
  {0x5B, 0x4F, 0x76, 0x06},
  {0xF1, 0x47, 0x73, 0x06},
  {0xF9, 0x87, 0x74, 0x06},
  {0x51, 0xFD, 0xCF, 0x17},
  {0xD5, 0x0C, 0x75, 0x06},
  {0x91, 0x06, 0x77, 0x06},
  {0x19, 0xBC, 0x73, 0x06},
  {0xF2, 0xEE, 0x77, 0x06}
};
```

Figure 9 shows the UID mapping configuration for Relay 1, which is assigned to users authorized to access Floor 2. The registered RFID card UIDs are stored in an array and used by the microcontroller to determine whether Relay 1 should be activated during the authentication process.

Figure 10. Relay 2 Mapping

```
// Relay 2
const byte relay2UIDs[12][4] = {
  {0x6E, 0x66, 0x76, 0x06},
  {0xF3, 0xB7, 0x75, 0x06},
  {0x5A, 0xBA, 0x73, 0x06},
  {0xD2, 0xA0, 0x76, 0x06},
  {0x91, 0x37, 0x73, 0x06},
  {0x6D, 0x91, 0x77, 0x06},
  {0x96, 0x53, 0x73, 0x06},
  {0x17, 0x34, 0x74, 0x06},
  {0xB9, 0x67, 0x77, 0x06},
  {0x3C, 0xBA, 0x75, 0x06},
  {0x13, 0x38, 0xE9, 0x34},
  {0xAC, 0x93, 0x76, 0x06}
};
```

Figure 10 shows the UID mapping configuration for Relay 2. This mapping enables the system to recognize RFID cards that

are granted access to Floor 3 and activate the corresponding relay output upon successful authentication.

Figure 11. Relay 3 Mapping

```
// Relay 3
const byte relay3UIDs[12][4] = {
  {0xF6, 0xF8, 0x74, 0x06},
  {0x32, 0x6C, 0x74, 0x06},
  {0x22, 0x0F, 0x77, 0x06},
  {0x74, 0x3B, 0x74, 0x06},
  {0x1C, 0x24, 0x76, 0x06},
  {0x4E, 0x85, 0x73, 0x06},
  {0xE9, 0xC5, 0x76, 0x06},
  {0x26, 0x9B, 0x77, 0x06},
  {0xFE, 0x6A, 0x74, 0x06},
  {0xF0, 0x8F, 0x7A, 0x5F},
  {0x3D, 0x37, 0x75, 0x06},
  {0xE6, 0xA7, 0x73, 0x06}
};
```

Figure 11 shows the UID mapping configuration for Relay 3, which is associated with access authorization for Floor 4. The stored UID data allows the microcontroller to identify eligible users and execute the appropriate elevator floor selection command.

C. Relay Activation Testing

Relay activation testing was conducted to verify that each registered RFID card could correctly trigger the relay corresponding to its assigned floor access level. The test results demonstrate the ability of the system to distinguish user authorization levels and activate the appropriate relay output.

Figure 12. Relay 1 Testing

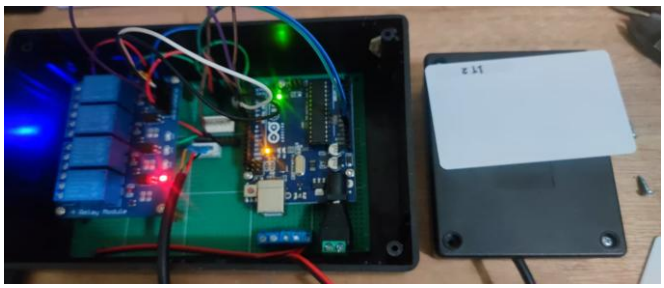


Figure 12 shows the testing result of Relay 1 activation. When an authorized RFID card assigned to Floor 2 is detected, the system successfully activates Relay 1 for the predefined duration, indicating proper operation of the authorization mechanism.

Figure 13. Relay 2 Testing

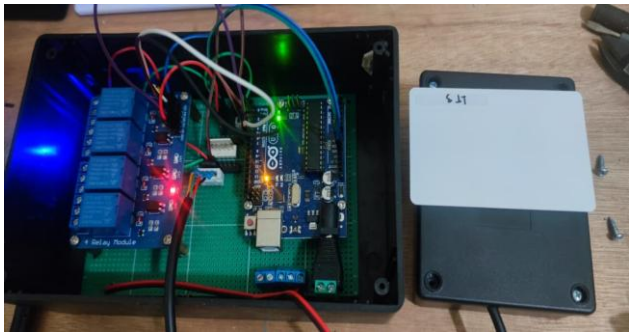


Figure 13 shows the testing result of Relay 2 activation using an RFID card registered for Floor 3 access. The relay responded according to the programmed access rights, demonstrating correct system functionality.

Figure 14. Relay 3 Testing

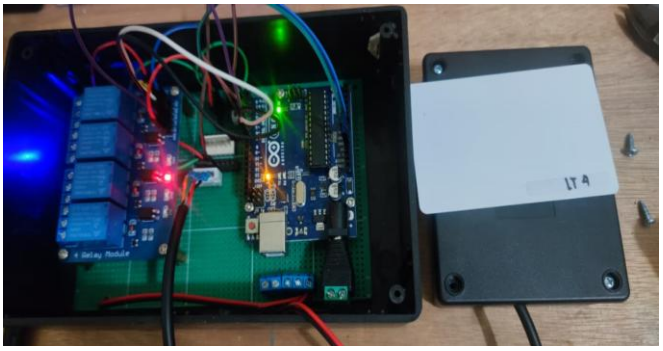


Figure 14 shows the testing result of Relay 3 activation. The relay was successfully triggered when an authorized RFID card associated with Floor 4 was presented to the RFID reader.

Figure 15. Master Card Testing

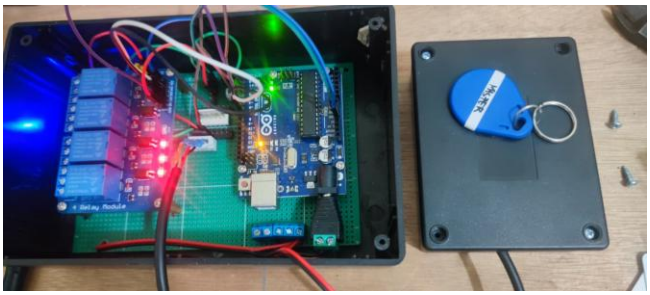


Figure 15 shows the testing result of the Master Card function. The system successfully recognized the registered master card and executed the corresponding administrative operation according to the programmed authorization rules.

D. RFID UID Registration Results

The UID data of the cards used in the system is stored directly in the Arduino program memory. With this approach, the system does not require external storage media, making the hardware structure simpler and more stable.

The number of cards registered in the program consists of:

1. 11 Master Cards
2. 12 Cards for Relay 1
3. 12 Cards for Relay 2
4. 12 Cards for Relay 3

Thus, the total number of UIDs registered in the system is 47 RFID cards.

D. Installation Process in the Elevator Panel

The RFID-based elevator authorization system was installed inside the elevator control panel after all hardware components had been assembled and verified through preliminary testing. The installation process was carried out by integrating the controller box with the existing elevator control circuit without modifying the original operating mechanism of the elevator. This approach ensures that the RFID system functions as an

additional access control layer while maintaining the safety and reliability of the existing elevator system.

Figure 16. Installation Process of the RFID-Based Elevator Authorization System

Figure 16 shows the installation process of the proposed RFID-based elevator authorization system inside the elevator control panel.

The relay wiring was implemented by connecting only the Normally Open (NO) contacts in parallel with the elevator push-button switches. This approach ensures that the RFID authorization system functions as an external access control interface without altering the original elevator circuitry, thereby maintaining the safety and operational reliability of the elevator.

Figure 17. Hardware Installation Inside the Elevator Control Panel

Figure 17 shows the completed installation of the RFID-based elevator authorization system inside the elevator control panel.

Figure 18. RFID Reader Installed on the Elevator Car Operating Panel (COP)

Figure 18 shows the RFID reader installed on the elevator Car Operating Panel (COP) as the primary user authentication interface. The reader is positioned below the floor selection buttons to provide convenient access while maintaining the original panel layout. Users are required to present a registered RFID card to the reader before selecting an authorized floor. Upon successful authentication, the corresponding relay is activated, allowing the selected elevator button to function according to the user's assigned access rights.

E. Results of the User Authorization System Testing

The results of user authorization testing using registered and unregistered RFID cards are presented in Table IV.

TABLE IV
USER AUTHORIZATION TEST RESULTS

No.	UID Category	Number of Registered UIDs	Access Rights	Activated Relay	Test Result
1	Master Card	11	Full access to all floors	1,2,3	Pass
2	Relay 1 Card	12	Access to Floor 2	1	Pass
3	Relay 2 Card	12	Access to Floor 3	2	Pass
4	Relay 3 Card	12	Access to Floor 4	3	Pass
5	Unregistered Card	2	No access		Denied

To evaluate the effectiveness of the proposed RFID authorization system, user authorization testing was conducted using registered and unregistered RFID cards. The test verifies whether each UID is correctly identified and assigned to its corresponding access level. The detailed testing results are presented in Table IV.

F. Authentication Response Time

The authentication response time measured at each processing stage of the proposed system is presented in Table V.

TABLE V
RESPONSE TIME ANALYSIS

No.	Process Stage	Duration
1	Accepted buzzer activation	200 ms
2	Rejected buzzer activation	800 ms
3	Relay activation period	3000 ms (3.0 s)
4	Anti double-scan interval	1500 ms (1.5 s)

Table V presents the predefined timing parameters implemented in the Arduino program. The accepted and rejected buzzer activation durations provide audible feedback for user authentication, while the relay activation period determines the time during which the selected elevator button remains enabled. Additionally, the anti double-scan interval prevents repeated card readings within a short period, thereby improving system stability during operation.

G. Measurement of Effective Reading Distance

The effective reading distance of the MFRC522 RFID reader is summarized in Table VI.

TABLE VI
EFFECTIVE READING DISTANCE MEASUREMENT

No.	Distance from Card to Reader (cm)	Detection Status
1	0	Detected
2	1	Detected
3	2	Detected
4	>3	Not Detected

The effective reading distance of the MFRC522 RFID reader was evaluated by measuring the maximum distance at which RFID cards could be consistently detected. This test was performed to determine the operational reading range of the proposed authorization system. The measurement results are summarized in Table VI.

H. Evaluation of Success Rate and Robustness

The overall performance and robustness evaluation results of the proposed RFID-based elevator authorization system are presented in Table VII.

TABLE VII
SUCCESS RATE AND ROBUSTNESS TEST RESULTS

No.	Test Parameter	Test Configuration	Successful	Failed	Success Ra
1	UID reading	10 × 4 Card	40	0	100%
2	UID verification	10 × 4 Ca	40	0	100%
3	Relay activation	10 × 4 Card	40	0	100%
4	Rejection of unregistered cards	5 × 2 Card	10	0	100%
5	Repeated scanning	10 × 4 Card	40	0	100%

To assess the overall reliability of the developed prototype, several performance and robustness tests were conducted under different operating conditions. The evaluation includes UID reading, authorization verification, relay activation, access rejection, and repeated scanning tests. The overall success rate obtained from these experiments is presented in Table VII.

IV. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

Based on the results of the design, implementation, and testing of the RFID-based elevator access control system, the following conclusions were drawn.

1. The developed system successfully implemented RFID technology as a user authentication method in the elevator access control system. The RC522 RFID module was able to accurately read the card's UID, while the Arduino Uno successfully processed the authentication data and controlled the relay according to the predetermined access rights.
2. The system is capable of distinguishing user authorization levels based on the RFID card UIDs stored in the Arduino's program memory. The system implementation consists of several access categories: master card, Relay 1 access card, Relay 2 access card, and Relay 3 access card. The master card has full access rights to activate all relays simultaneously, while standard user cards can only activate relays corresponding to the designated floor.
3. The relay control mechanism works effectively using a non-blocking timer method based on the millis() function. Each relay remains active for approximately 3 seconds before automatically returning to the inactive state. This method allows multiple relays to be active simultaneously without interfering with the RFID reading process.
4. The buzzer system, serving as an audio indicator, successfully provides notifications regarding authentication results. Registered cards produce a brief confirmation sound, while unregistered cards produce a warning sound to indicate that access has been denied.
5. Based on system testing results, the developed prototype demonstrated stable performance with a 100% success rate in UID reading, access verification, relay activation, and rejection of unregistered cards. Additionally, the RC522 RFID module has an effective reading range of up to approximately 2 cm under normal operating conditions.

Overall, the designed system has successfully achieved the research objectives outlined in the proposal, namely to design and implement an RFID-based elevator access control system capable of restricting user access based on specific authorization levels

B. Recommendation

Although the developed system operated successfully, several improvements can still be implemented in future development stages.

1. The system can be enhanced by integrating a database or cloud-based storage system to support dynamic UID management without requiring firmware modification.
2. The security level can be further improved by

implementing encrypted communication or multi-factor authentication methods in addition to RFID technology.

3. The prototype may be expanded to support a larger number of floors and relay outputs for application in multi-story buildings with more complex access requirements.
4. A dedicated PCB design and industrial-grade power supply are recommended for long-term deployment to improve system durability, electrical stability, and installation reliability.
5. Future studies may evaluate system performance under real operational environments, including high user traffic conditions, electromagnetic interference, and continuous long-term operation.

These recommendations are expected to support the further development of a more secure, scalable, and reliable elevator access control system in practical applications.

ACKNOWLEDGMENT

The author offers praise and thanks to God Almighty, for through His grace and blessings, this research titled "RFID-Based Elevator Access Control System" has been successfully completed.

The author extends his deepest respect and gratitude to Mr. Vivin Octowinandi, the academic advisor, and all faculty members at Batam State Polytechnic for providing guidance, direction, support, and invaluable feedback throughout the research process and the preparation of this journal article. The knowledge, experience, and attention provided served as a major motivation for the author in completing this research.

The author also extends gratitude to family and friends who provided support, motivation, and assistance throughout the design, testing, and completion of the research.

Furthermore, the author thanks all parties who assisted, either directly or indirectly, in ensuring this research was successfully completed.Publishing Policy and Plagiarism

REFERENCES

[1] S. R. Kishan, S. Hameed, J. Charan, and Y. Srikar, "RFID-Based Elevator Access Control System," in Proc. 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, Jun. 2024, doi: 10.1109/ICCCNT61001.2024.10724057.

[2] A. Mohankumar, I. Ahamath, and G. R., "Revolutionizing Home Security: A Comprehensive Overview of an Advanced RFID Door Lock System for Keyless Access and Smart Home Protection,"
Asian Journal of Applied Science and Technology (AJAST), vol. 8, no. 1, pp. 1–13, Jan.–Mar. 2024.

[3] L. Islam, M. B. A. Z. Shammo, and M. I. Hossain, "Real-Time RFID Authentication and Access Control System with Networked Logging," 2025.

and Technology (AJAST), vol. 8, no. 1, pp. 1–13, Jan.–Mar. 2024.

[4] I. F. Firmansyah, N. Supriatna, and R. Kurniawan, "Implementasi Sistem RFID RC522 Untuk Pemantauan Inventaris Lab Komputer Berbasis Arduino," *Jurnal Informatika, Robotik dan Sistem Informasi (JIRSI)*, vol. 1, no. 2, pp. 45–53, 2024.

[5] 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

and Technology (AJAST), vol. 8, no. 1, pp. 1–13, Jan.–Mar. 2024.

[6] A. Ramzan, W. Farhan, I. Malahat, and N. Afzal, "Double-Layered Authentication Door-Lock System Utilizing Hybrid RFID-PIN Technology for Enhanced Security," *Materials Proceedings*, vol. 23, 2025, doi: 10.3390/materproc2025023019.

[7] A. Babii and A. Samila, "Dual Authentication Technique for RFID Access Control Systems with Increased Level of Protection," *Systems, Information Technologies and Control*, vol. 1, no. 1, pp. 1–8, 2023, doi: 10.31861/sisiot2023.1.01011.

[8] M. Galina, A. Tambunan, H. Situmorang, and M. Siahaan, "Multi-Security System Based on RFID, Fingerprint and Keypad Authentication," *ELKHA: Jurnal Teknik Elektro*, vol. 14, no. 2, pp. 125–131, Oct. 2022.

[9] S. Mustafa, M. Khaidir, M. Ikhsan, M. I. Kido, and M. Fachrul, "Rancang Bangun Prototype Sistem Pintu Otomatis Berbasis ATmega328P," *Jurnal Tematis (Teknologi, Manufaktur dan Industri)*, vol. 5, no. 1, pp. 58–61, 2023.

[10] I. D. Akrimni, D. R. Akbi, and Z. Sari, "Rancang Bangun Pintu Otomatis Berbasis Arduino RFID dan Voice Recognition Arduino," *REPOSITOR*, vol. 6, no. 1, pp. 17–26, Feb. 2024.

[11] M. Fauza and M. A. Muthalib, "Sistem Pengaman Pintu Otomatis Menggunakan Sensor Radio Frequency Identification (RFID) Berbasis Arduino Uno," *Jurnal Energi Elektrik*, vol. 11, no. 1, pp. 30–37, 2022.

[12] E. A. P. Marpaung, D. C. P. Sinaga, R. F. Siahaan, R. H. Lubis, and D. N. Amalliaendra, "Sistem Pengamanan Pintu Otomatis Menggunakan RFID RC522 Berbasis Mikrokontroler Arduino," *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, vol. 8, no. 2, 2025.

[13] I. Muzaki, M. I. Amal, and M. Alfarisi, "Smart Lock Door Menggunakan RFID RC522 Berbasis Microcontroller Arduino Nano," *TRANSIENT: Jurnal Ilmiah Teknik Elektro*, vol. 13, no. 2, pp. 75–81, Jun. 2024.

[14] A. Vel'as, M. Boroš, R. Kuffa, and F. Lenko, "Testing of Permeability of RFID Access Control System for the Needs of Security Management," *Applied Sciences*, vol. 14, no. 10, p. 4227, 2024, doi: 10.3390/app14104227.

[15] I. Rusten-Andrei, "Design of an Arduino-Based Intelligent Access Control System Using Multi-Factor Authentication," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, 2025.