



# Design and Build Entry Access Restriction System Laboratory Using Radio Frequency Identification (RFID) and Keypad Technology

Ahmad Aziz Arrizal\*, Sri Wahyu Suciayati, Arif Surtono, and Gurum Ahmad Pauzi

Department of Physics, University of Lampung, Bandar Lampung, Indonesia, 35141

## Article Information

*Article history:*  
Received December 27th, 2021  
Received in revised form December 30th, 2021  
Accepted December 30th, 2021

**Keywords:** Arduino Mega, Keypad, RFID, Solenoid Lock

## Abstract

*The laboratory access restriction system has been realized using RFID and keypad technology, based on an Arduino microcontroller as a processor. The system has recorded users who entered the room by identifying the RFID tag (transponder) used to open the door from the outside. As for access outside the room, the user only needs to enter the password as identification data on the keypad, and the system would reduce the number of room users and open the door. The output of this system was a solenoid lock which functions as an electronic lock and an LCD to display the status of the RFID reading. The test results showed that the system created can work well. RFID Reader was able to read tags with a maximum distance of 4 cm. The program counter functions well, so the number of users was limited to 15 (50% of the maximum capacity).*

## Informasi Artikel

*Proses artikel:*  
Diterima 27 Desember 2021  
Diterima dan direvisi dari 30 Desember 2021  
Accepted 30 Desember 2021

**Kata kunci:** Aduino Mega, Keypad, RFID, Solenoid Lock

## Abstrak

*Sistem pembatas akses ruangan laboratorium telah direalisasikan menggunakan teknologi RFID dan keypad berbasis mikrokontroler Arduino sebagai pemroses. Sistem mendaftarkan pengguna yang masuk ruangan dengan cara mengidentifikasi tag (transponder) RFID yang digunakan untuk membuka pintu dari luar, sedangkan untuk akses keluar ruangan, pengguna cukup memasukkan password sebagai data identifikasi pada keypad maka sistem akan mengurangi jumlah pengguna ruangan dan pintu terbuka. Hasil keluaran dari sistem ini berupa solenoid lock yang berfungsi sebagai pengunci elektronik dan LCD untuk menampilkan status pembacaan RFID. Hasil pengujian menunjukkan bahwa sistem yang dibuat dapat bekerja dengan baik. Program counter berfungsi dengan baik, sehingga jumlah pengguna pada sistem ini dibatasi sebanyak 15 pengguna (50% dari kapasitas maksimal). RFID Reader mampu membaca Tag dengan jarak maksimal 4 cm.*

## 1. Introduction

The need to carry out social and physical distancing to stop the spread of Coronavirus Disease 2019 (Covid - 19) makes the world of education unable to carry out short-distance educational activities (Darmawan et al., 2020). It also affects educational activities such as research and practicum, which can only be done in the laboratory. The laboratory is a place to carry out various practicum activities, research, observation, training, and scientific testing as an approach between theory and practice from various disciplines (Decaprio, 2013). One way to prevent the spread of Covid-19 is to limit the use of space to a maximum of 50% (fifty percent) of the occupancy capacity of the room/class/laboratory and a maximum of 25 (twenty-five) people (Nizam, 2021). Therefore, we need a technology that can be used on the door as a laboratory access system to maintain security and limit the number of laboratory users.

The technology that can be applied to doors as laboratory access systems is electronic devices that function as electronic locks. According to Ramady & Juliana (2019), electronic locks are more efficient and secure than conventional locks. Some of the applications of the technology used as an access tool or electronic key input such as

\* Corresponding author.  
E-mail address: ahmadazizarrizal@gmail.com

smart cards (smartcards) (Tawakal & Ramdhani, 2021), passwords or Personal Identification Numbers (PIN) (Suwartika & Sembada, 2020), QR code (Hazarah, 2017), fingerprint (Febriyanto, Padeli, & Suprayogi, 2019; Simanihuruk, 2020), voice (Prakasa, 2017), temperature (Margarini, Suciayati, Surtono, & Pauzi, 2021) up to face detection (Sandar & Oo, 2019). Electronic lock technology that can be easily applied to laboratory doors to limit and secure and identify users is a smart card. Card reader technology currently being developed as a fundamental electronic model with data identification method is Radio Frequency Identification (RFID).

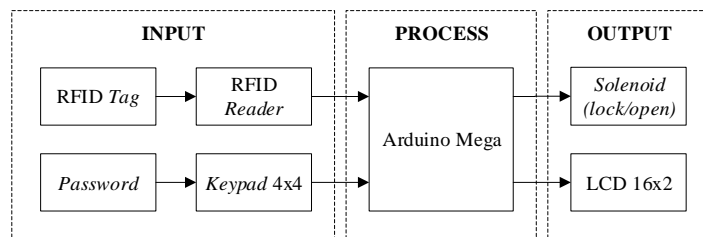
Research on RFID that has been carried out includes a door security system using e-KTP and PIN. E-KTP is included in the type of smartcard that can be operated electronically through an RFID reader as an informed reader. The addition of PIN input as a second level of security to anticipate the possibility of misuse of e-KTP by others for access to enter the room while opening the door from inside and out of the room is enough to use a push-button. (Wendanto, Salim, & Putra, 2019). However, there is no limit to the number of people using the room.

Develop a security system from previous research, namely by limiting the number of room users and registering users who access the door. Based on the description above, research has been carried out on designing a laboratory access barrier system using RFID and keypad technology. The system records users who enter the room by identifying the RFID tag (transponder) used to open the door from the outside. As for access outside the room, the user only needs to enter the password as identification data on the keypad, and the system will reduce the number of room users and open doors.

## 2. Research Methods

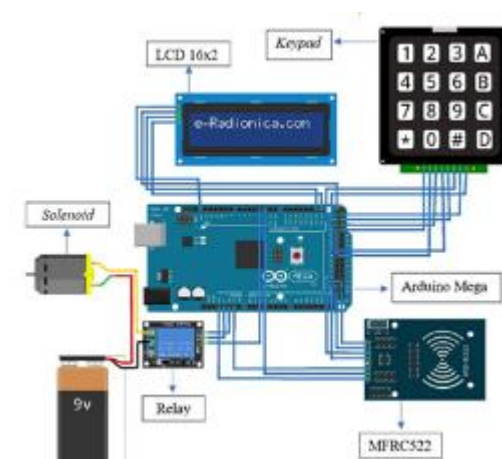
The tools and materials used in this research are, *Personal Computer (PC)*, *power supply*, *soldering iron*, *multimeter*, *Arduino Mega* and *Arduino IDE*, *solenoid lock module*, *MFRC 522 RFID reader* and *RFID tag*, *4x4 keypad*, *5V relay*, *16x2 LCD*, *jumper*s and *acrylic*.

The design of the entry access barrier system in this study is to connect the MFRC522 RFID reader, 4x4 keypad, solenoid lock, and 16x2 LCD with the Arduino board. The RFID reader MFRC522 as a room entry access sensor, functions to read and identify tags and match the RFID data stored in the program. Keypad 4x4 as an opener to access the room serves to identify the entered password. Furthermore, as a programmed processor, Arduino will give orders to the system to activate the relay to apply voltage to the solenoid lock so that the access system is open. In comparison, the 16x2 LCD is a data viewer whether the tag can access the barrier system or not. The block diagram of this system is shown in **Figure 1**.



**Figure 1.** Block diagram of how the tool works.

Based on the block diagram in **Figure 1**, the overall circuit needed to manufacture the tool is shown in **Figure 2**. The MFRC522 reader is used to read or detect nearby RFID tags. After that, the counter will count the number of users accessing the room divider system.



**Figure 2.** The overall circuit of the access barrier system.

MFRC522 has eight pins on the reader, 5 of which are connected to the Arduino Mega digital pin, one pin for ground, and one pin for power / VCC. The configuration of the MFRC522 pin reader with Arduino is shown in **Table 1**.

**Table 1.** MFRC522 Pin Configuration with Arduino.

No.	MFRC522 Pin Pins	Arduino Pins
1	natural resources	D 52
2	SCK	D 5 3
3	MOTION	D 51
4	MISO	D 50
5	IRQ	-
6	GND	GND
7	RST	D9
8	3.3 V	VCC 3.3V

The 16x2 LCD is used as an *interface* to display the *standby condition of the device* and when the device reads input from the MFRC522. The 16x2 LCD used is equipped with an I2C module, so it only requires four pins connected to Arduino. In the circuit shown in **Figure 2**, it is shown that the LCD has been equipped with an I2C module, so it only requires four pins to be connected to Arduino. The Arduino pin configuration with an LCD equipped with an I2C module is shown in **Table 2**.

**Table 2.** LCD Pin Configuration with Arduino.

No.	The pin I2C	Arduino
1	natural resources	D20
2	SCL	D21
3	GND	GND
4	VCC	VCC 5V

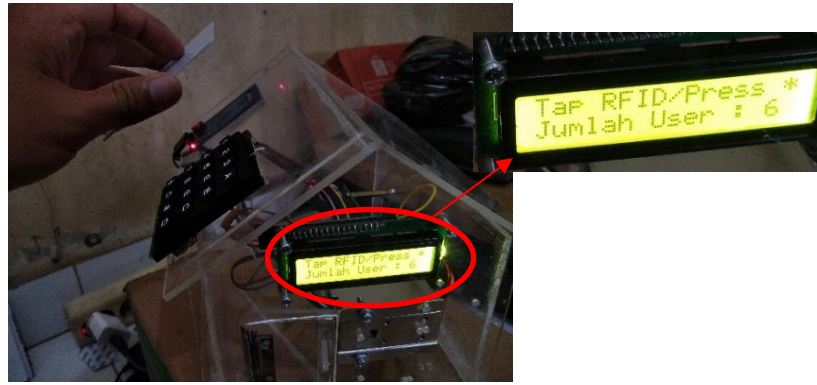
### 3. Results and Discussions

The room restriction system limits the number of users by 50% of the capacity. The realization of the room access barrier system is shown in Figure 3. The system consists of 2 main parts: the entry access control system using RFID sensors and the outgoing access control system using the *keypad*. The hardware in this barrier system is a series of RFID readers, a series of *keypads*, and an Arduino microcontroller. The RFID reader circuit, as a room entry sensor, serves to identify *the tag* and match it with the RFID data stored in the program. The series of *keypads* as opening access to the exit door serves to identify the entered password with *the password* stored in the program. The Arduino microcontroller processes the sensor input results to control *the relay* to give or not apply voltage to the *solenoid lock* so that the door lock will open or close the room access. The software functions to read and match data from RFID sensor readings and n a *keypad* with data stored in the program, which will then give an order to activate the *solenoid lock* so that the access to the room door lock will open and count the number of visitors, then display the number of visitors on the LCD.



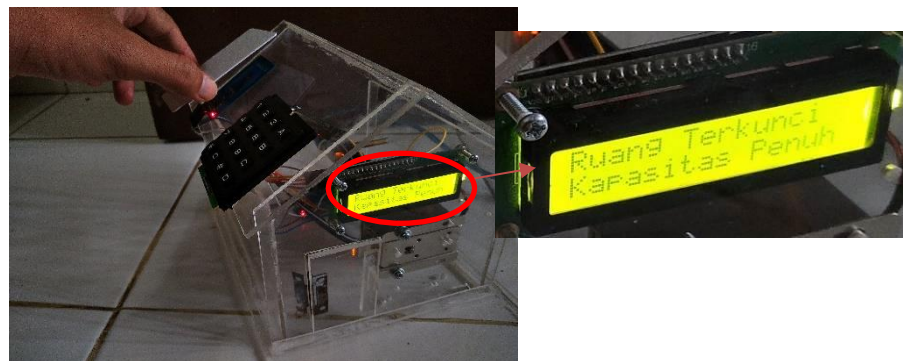
**Figure 3.** Access barrier system with RFID and *keypad*.

The characteristics of the MFRC522 module are known after testing the readings by the MFRC522 *reader* with and without barriers. *The counter* data retrieval that has been carried out is shown in Figure 4. The counter is running successfully when access is entered via RFID scanning, and the maximum limit is 15 users, assuming the maximum number of laboratory capacities before being limited is 30 people.



**Figure 4.** Retrieval of counter data.

After reaching 15 users, room access will be closed and reopened if anyone leaves the room using a *password* on the *keypad*, reducing *the counter*. Data retrieval when it has reached 15 users that have been carried out is shown in **Figure 5**.



**Figure 5.** Data retrieval at total capacity.

When the number of users has reached the maximum limit (15 users), and some users want to enter, the access will be denied, the door will be locked, and the LCD will display the message 'Locked Room, Full Capacity' as shown in **Figure 5**.

### 3.1 Barrier-free MFRC522 Reader Test

The test aims to determine the reading distance and the ability to pass through barriers that the MFRC522 RFID reader can reach. The reading distance test was carried out ten times at each distance by bringing the tag and reader closer together in a parallel position. The tag is brought close to the reader slowly from a distance of 10 cm to 0 cm, then see the response whether the reader has read the tag by paying attention to the serial monitor. If the tag is read, the serial monitor will display the *tag's ID*. The results of the MFRC522 reader test data are shown in **Table 3**.

**Table 3.** Reader reading distance capability.

No	Distance (cm)	Description (0 = unreadable; 1 = legible)									
		data to-									
		1	2	3	4	5	6	7	8	9	10
1	10	0	0	0	0	0	0	0	0	0	0
2	9	0	0	0	0	0	0	0	0	0	0
3	8	0	0	0	0	0	0	0	0	0	0
4	7	0	0	0	0	0	0	0	0	0	0
5	6	0	0	0	0	0	0	0	0	0	0
6	5	0	0	0	0	0	0	0	0	0	0
7	4	1	1	1	1	1	1	1	1	1	1
8	3	1	1	1	1	1	1	1	1	1	1
9	2	1	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	1	1	1

**Table 3** shows that the reader is capable of reading/detecting *tags up to a distance of 4 cm*. At a distance of 5 to 10 cm, the *reader can no longer detect/read the tag*.

### 3.2 MFRC522 Reader Test with Barrier

The next test is the *reader's reading* when given a barrier. This aims to determine the *reader's reading ability* when blocked by objects with certain materials. The perimeter of the barrier used is the circumference of the tag so that the barrier will completely cover the entire part of the *tag*. The thickness of the barrier used varies, but the distance between the tag and the reader is uniform, with the *reader's reading ability* without a barrier which is 4 cm. The RFID test data using the barrier is shown in **Table 4**.

**Table 4.** RFID test data with barrier.

No.	Barrier Type	Barrier thickness(mm)	Description (0 = unreadable; 1 = legible)				
			data to-				
			1	2	3	4	5
1	Acrylic	5	1	1	1	1	1
2	multiplex	15	1	1	1	1	1
3	Leather Wallet	5	1	1	1	1	1
4	Iron Plate	1	0	0	0	0	0

Based on the data in **Table 4**, at a distance of 4 cm with a barrier, the reader can read/detect the types of barriers made of acrylic, multiplex, and leather wallets. While the barrier with an iron plate, the reader is not able to read. The *datasheet* explains that the scanning distance capability can reach a distance of 10 cm with a voltage of 3.3 V. The reading distance in this study is only able to read as far as 4 cm, even though the reading distance is as far as 4 cm. is good enough, because *the tags* used are passive.

### 3.3 RFID testing and counter ++

This test tests the *counter ++* program when the user accesses the room door lock using a *tag* that is brought close to the *reader*. If the registered *tag* is brought closer to the *reader*, the desired response is that the door lock access will open, and the *counter variable* will increase by 1. The *counter* will continue to increase until it reaches 15 users. After the number of users in the room reaches the maximum, the system will stop *counter ++*, and door lock access will be closed. The RFID and *counter ++* testing results are shown in **Table 5**.

**Table 5.** RFID testing and *counter ++*.

data to-	UID	Registered/Not	Counter ++	Information
1	214,125,135,30	Yes	Yes	Open door, <i>counter</i> + 1
2	170,73,101,67	Yes	Yes	Open door, <i>counter</i> + 1
3	25,27,100,67	Yes	Yes	Open door, <i>counter</i> + 1
4	23,59,100,67	Yes	Yes	Open door, <i>counter</i> + 1
5	54,64,100,67	No	No	The door is locked, and the <i>counter</i> does not increase

**Table 5** shows that the registered *tag* can open the door lock access and instruct the *counter program* to increase the variable by 1. Thus, *counter ++* is working well and can then be used to limit room access when the room visitors have reached 15 people.

### 3.4 Password and counter testing --

*Password* testing aims to test the suitability of the input *password keypad* with *passwords* stored in the Arduino program. User *password* testing data is shown in **Table 6**.

**Table 6.** Testing data for user/user *passwords*.

data to-	Password	True False	Counters --	Information
1	0000	Right	Yes	Open door, <i>counter</i> - 1
2	1234	Wrong	No	The door is locked, the <i>counter</i> is fixed
3	0124	Wrong	No	The door is locked, the <i>counter</i> is fixed
4	0114	Wrong	No	Doors locked, <i>counters</i> fixed. The user waits 30 seconds before entering the <i>password</i> again
5	0000	Right	Yes	Open door, <i>counter</i> - 1

data in **Table 6** shows the compatibility between the buttons on the *keypad* and the *passwords* stored in the program. When the *password* is entered correctly, access will be accepted, and the room door lock will open, then the *counter* on the program will decrease by 1. On the other hand, if the *password* is entered incorrectly, access will be denied, and the door lock will not open. When the user enters the wrong *password* three times in a row, the door will be locked for 30 seconds before being able to enter the *password* again.

#### 4. Conclusions

Based on the realization of the research and analysis that has been carried out, it is concluded that room access restrictions can be realized using RFID and *keypads*, restrictions on the number of accesses using the program *counter* function properly, so that the number of users on this system is limited to 15 users (50% of the capacity). maximum) Moreover, RFID can read *tags* up to a maximum distance of 4 cm.

#### 5. Bibliography

- Darmawan, J., Andriani, A., Usnila, R., Ledy, K., Fitria, Y., Armanawi, & Bakhtiar. (2020). *Praktik Baik Masa Pandemi*. Sukabumi-Jawa Barat: CV. Jejak.
- Decaprio, R. (2013). *Tips Mengelola Laboratorium Sekolah*. Yogyakarta: Diva Press.
- Febriyanto, E., Padeli, & Suprayogi, D. (2019). Prototype Sistem Smart Lock Door dengan Timer dan Fingerprint Sebagai Alat Autentikasi Berbasis Arduino Uno pada Ruangan. *Jurnal Informatika*, 19(1), 10–19.
- Hazarah, A. (2017). Rancang Bangun Smart Door Lock Menggunakan QR Code dan Solenoid. *Jurnal Teknologi Informatika Dan Terapan*, 04(01), 5–10.
- Margarini, D., Suciati, S. W., Surtono, A., & Pauzi, G. A. (2021). Rancang Bangun Prototipe Keamanan Ruang Laboratorium dengan Pintu Otomatis Menggunakan Sensor Suhu MLX90614 Berbasis Arduino Atmega 2560. *Journal of Energy, Material, and Instrumentation Technology*, 2(4), 69–77.
- Nizam. Surat Edaran Nomor 4 Tahun 2021 Tentang Penyelenggaraan Pembelajaran Tatap Muka Tahun Akademik 2021/2022 (2021). Jakarta: Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi.
- Prakasa, G. N. (2017). *Prototipe Kunci Pintu Menggunakan Motor Stepper Berbasis Arduino Mega 2560 dengan Perintah Suara pada Android*. Bandar Lampung: Universitas Lampung.
- Ramady, G. D., & Juliana, R. (2019). Sistem Kunci Otomatis Menggunakan RFID Card Berbasis Mikrokontroler Arduino Uno R3. *ISU Teknologi STT Mandala*, 14(1), 28–32.
- Sandar, S., & Oo, S. A. N. (2019). Development of a Secured Door Lock System Based on Face Recognition using Raspberry Pi and GSM Module. *International Journal of Trend in Scientific Research and Development - IJTSRD*, 3(5), 357–361.
- Simanihuruk, F. N. (2020). *Rancang Bangun Pengaman Pintu Otomatis Menggunakan E-KTP dan Sidik Jari (Fingerprint FPM 10A) Berbasis SMS Gateway*. Medan: Universitas Sumatera Utara.
- Suwartika, R. K., & Sembada, G. (2020). Perancangan Sistem Keamanan Menggunakan Solenoid Door Lock Berbasis Arduino Uno pada Pintu Laboratorium di PT. XYZ. *Jurnal E-KOMTEK (Elektro-Komputer-Teknik)*, 4(1), 62–74.
- Tawakal, M. I., & Ramdhani, Y. (2021). Smart Lock Door Menggunakan Akses E-KTP Berbasis Internet of Things. *Jurnal Responsif*, 3(1), 83–91.
- Wendanto, W., Salim, D. J. N., & Putra, D. W. T. (2019). Rancang Bangun Sistem Keamanan Smart Door Lock Menggunakan E-KTP ( Elektronik Kartu Tanda Penduduk ) Dan Personal Identification Number Berbasis Arduino Mega R3. *Go Infotech: Jurnal Ilmiah STMIK AUB*, 25(2), 133–142.