Journal of Applied Science, Engineering and Technology
e-ISSN: 2722-8363 p-ISSN: 2722-8371
DOI: 10.47355/ASET.V1I2.12

J. ASET

Radio Frequency Identification (RFID)-based of the Validated Electronic Lock for Automatic Monitoring System

S D Saputra[1], S Alam[1], S Purwiyanti[1], E Nasrullah, and, A S Repelianto[1],*

[1] Department of Electrical Engineering, Faculty of Engineering, Universitas Lampung, Jl. Prof. Soemantri Brojonegoro no. 1, Bandar Lampung, Indonesia 35145

* Correspondence: ageng.sadnowo@eng.unila.ac.id

Received: 17.08.2021; Accepted: 30.10.2021; Published: 31.12.2021

Abstract: This study aims to create a prototype of an electronic key system using internet of things-based for RFID with a validated monitoring system with registered data. This system is applied to the door of the integrated laboratory in the university. The electronic keys that are created are very difficult to break into and also easy to change the access secret code to maintain confidentiality. The developed electronic door lock device has strong security reliability with code validation. The code validation block serves as a door unlocks determinant. The validated data will produce a signal 1 which will drive the actuator, in this case the door lock solenoid, to work (lock open). The security code has 2554 combinations. To access the door from outside, the RFID tag should be registered in the database and permitted by administration and the ID number data is on the processor. The counter will count the number of people who pass through the door, if more than one person then the buzzer will sound. Then the door lock solenoid is closed and will lock the door again. From the experimental results it is found that this system can work well with a minimum delay of 1.8 s obtained at a distance between devices of 5 m.

Keywords: electronic lock; validated code; radio frequency identification; monitoring system

1. Introduction

Access to enter the Integrated Laboratory of the Department of Electrical Engineering (LTJTE) at the university is currently very open to the public. There is no special security at the main entrance. The main entrance only has a regular mechanical lock. It is vulnerable to breaches such as key duplication and others. Meanwhile, student activity at night to use the laboratory is quite high. Is is important to increase the concern of lab's security from the entry of unauthorized persons.

The importance of increasing security access for LTJTE building is an urgent demand, so that unwanted interference events can be prevented and even eliminated. To overcome these problems, it is necessary to make an electronic key that has a high level of security to avoid burglary. At the same time, it is also easy to change the access secret code to maintain the security. Therefore, this study aims to create an electronic security system that is applied to the main entrance of the LTJTE using Radio Frequency Identification (RFID) RC522 with the NodeMCU ESP8266 microcontroller based on the internet of things (IoT) [1].

The use of RFID as an electronic key has been developed in many applications with different validation methods. The validation method used can be in the form of a pin on the button [2], using an Indonesian residential identity card (E-KTP) and integrated with an RFID tag or keypad [3,4]. In a

simple term, the three studies above have the same design concept, as shown in Figure 1. The RFID sensor will check the RFID number through the ID tag, then the processor will determine whether the code is appropriate, and then activate the actuator to open the door [4].

Figure 1. The RFID concept for electronic locking system

This study modifies the previous concept, namely in the code validation process. Code validation is the final decision-making process from input tag ID code and database code sets [5]. In this case there is a database that will regulate whether someone is allowed to log in or not. The database is located in the administration room and is connected to the processor via the internet [6]. If the two codes have the same value, the processor will activate a signal to move the door lock actuator [7]. The developed electronic door lock device has strong security reliability with code validation. Which has 2554 combinations [8].

2. Materials and Methods

2.1 Materials

The design is made using tools and materials as described below. NodeMCU ESP8266 is used as a processor to process signals. RFID reader RC522, and RFID tag 13.56 MHz are used as transmitter and responder of the RFID system. Ultrasonic Sensor HC-SR04 to count people entering the laboratory door, Solenoid Door Lock 12V to lock and open the door with a 12V Single Channel Relay to disconnect the current to the door solenoid. Buzzer SFM-27 5V is useful as an alarm that sounds when people entering the door do not comply with the provisions. As for the software, Arduino IDE software version 1.8.5 is used to upload programs to the microcontroller and Blynk Software version 2.27.31 for internet applications.

2.2. Method

The system design concept used in this study is shown in Figure 2.

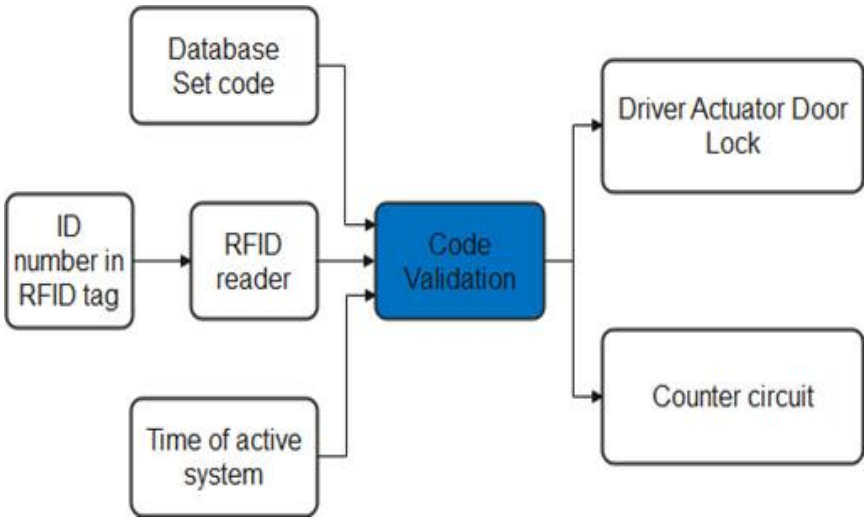

Figure 2. System concept

The code validation block serves as a door unlocks determinant. When the validation process produces signal 1, the signal will activate the actuator, in this case the door lock solenoid, to work (open lock) [9]. The validation signal will also activate the counter for people who pass through the door [10]. This circuit uses an ultrasonic sensor. The circuit will detect people passing through the door, if more than one is detected, the buzzer will sound, indicating more than one person passing through the door.

2.3. System Flowchart

The steps taken in the system to access the door from the outside can be represented in a flow diagram as shown in Figure 3.

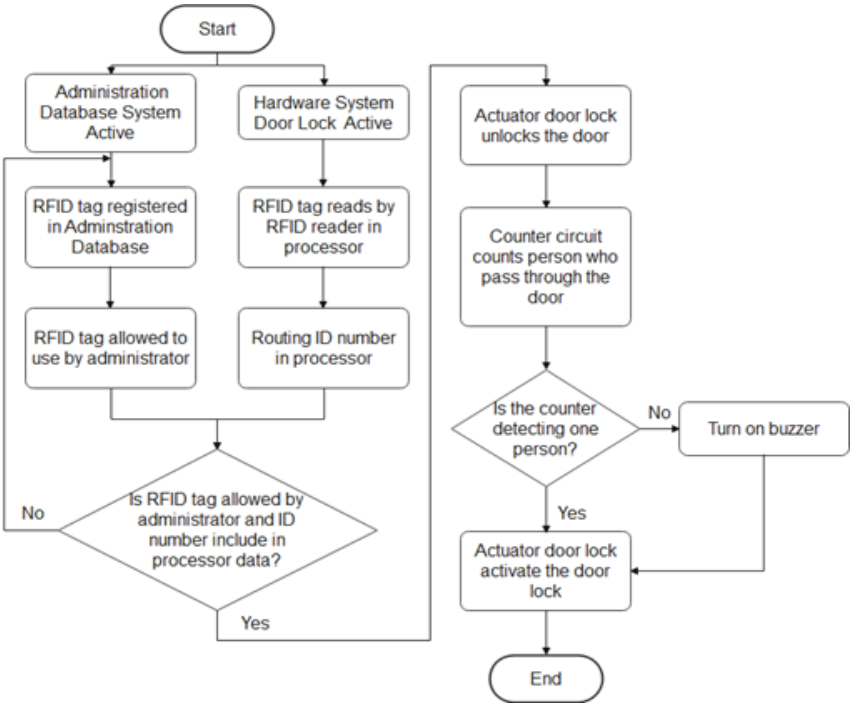

Figure 3. System flowchart

Figure 3 shows a flow diagram of the system for accessing the door from the outside. After the system is activated, the RFID tag registered in the database must be authorized by the administrative staff so that the RFID tag can be read by the RFID reader [11]. After that, the RFID reader will read the RFID tag and search for ID number data on the processor. If the ID number data is not contained in the processor and the RFID tag is not authorized by the administration, it will loop again [12]. If the RFID tag registered in the database is permitted by administration and the ID number data is on the processor, the door lock actuator, namely the door lock solenoid, will open. The counter will then count the number of people who pass through the door, if more than one person then the buzzer will sound. Then the door lock solenoid is closed and will lock the door.

The steps carried out in the system to access the door from the inside can be represented in a block diagram as shown in Figure 4. To access the system from inside, as shown in Figure 4, when a person is detected by the ultrasonic sensor, the data will be processed by the processor and the door lock solenoid is open. The counter circuit will count the number of people who pass through the door, if more than one person then the buzzer will sound then the door lock solenoid is closed and will lock the door.

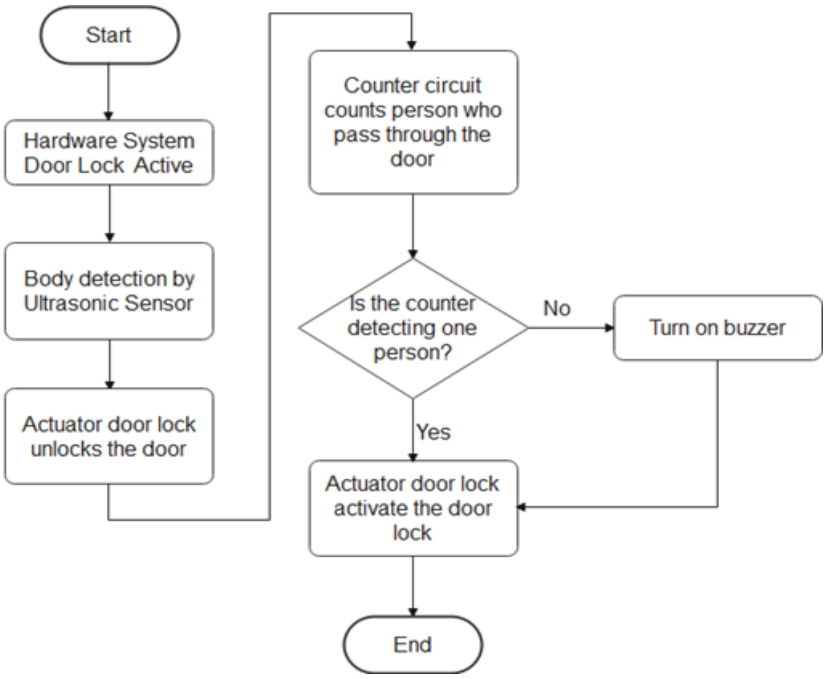

Figure 4. Flowchart for accessing from inside

2.4. System Block Diagram

The steps taken in the system to access the door from outside is represented in a block diagram as shown in Figure 5.

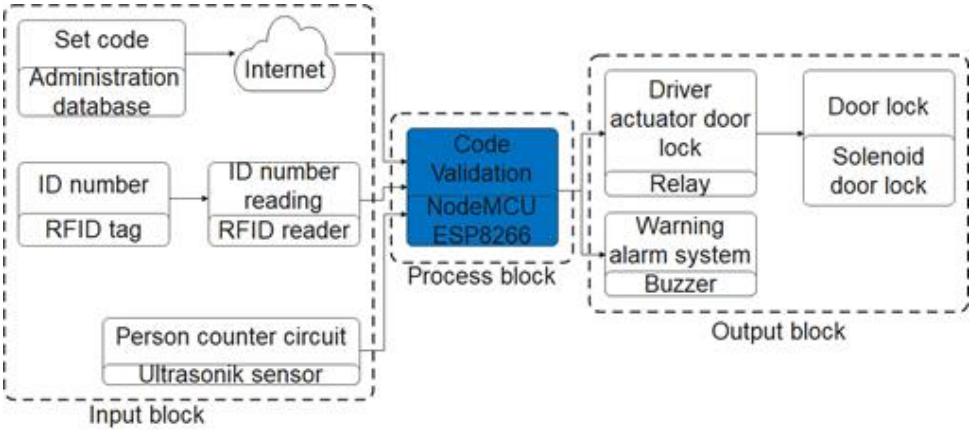

Figure 5. Flowchart for accessing from outside

To be able to enter the laboratory, there are two things that must be met, namely the RFID code is registered in the database and there is permission from the administrative staff to enter the laboratory. This is intended to avoid access from people who are not expected. In addition to the RFID tag registered in the database in the administration section, to be able to use it, permission is still needed from the administration so that the RFID tag can be read by the RFID reader [13]. Therefore, there are two conditions for an RFID tag to be allowed, namely being registered and obtaining permission. If the RFID tag is registered in the database in the administration section and is allowed by the administration, the RFID reader will be able to read it and the processor will do the routing to look up the ID number on the processor [14]. An explanation of code validation can be seen in Figure 6.

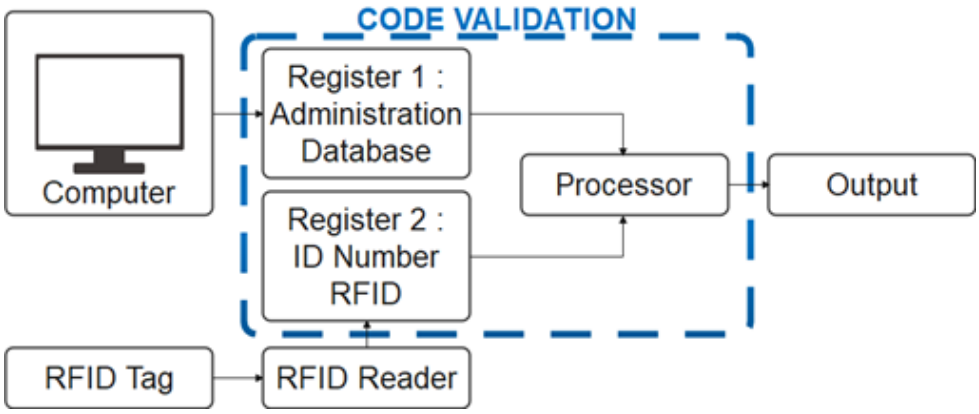

Figure 6. Code validation diagram

In Figure 6, it can be seen that the processor generates a signal based on input from the administrative database and data on the processor. Database input can be regarded as a set of code and data on the processor as a key code [15]. In this case, the processor will generate a signal of 1 only if the database and data on the processor have the same value, i.e., both are 1 or both are 0, as presented by others [15,16]. Next, the door lock solenoid will open. Then the counter will count the number of people who pass through the door, if more than one person then the buzzer will turn on. Subsequently the door lock solenoid is closed and will lock the door. The steps carried out in the system to access the door from the inside can be represented in a block diagram as shown in Figure 7.

In Figure 6 it can be seen that the processor generates a signal based on input from the administrative database and data on the processor. Database input can be regarded as a set of code and data on the processor as a key code. In this case, the processor will generate a signal of 1 only if the database and data on the processor have the same value, i.e., both are 1 or both are 0 [16]. Next, the door lock solenoid will open. Then the counter will count the number of people who pass through the door, if more than one person then the buzzer will turn on. Subsequently the door lock solenoid is closed and will lock the door.

The steps carried out in the system to access the door from the inside can be represented in a block diagram as shown in Figure 7.

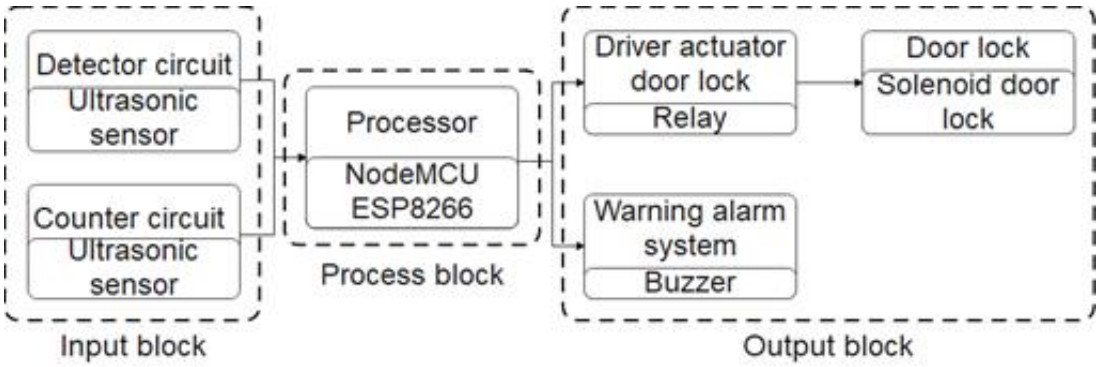

Figure 7. Block diagram of access system from within

The input is in the form of readings from the person detection circuit which will activate the actuator controller driver to unlock the door. The counter will count the number of people who pass through the door. If more than one person is detected, the buzzer will light up and the door lock solenoid will close and lock the door.

2.5. System Design

The position of the system at the door is described in Figure 8.

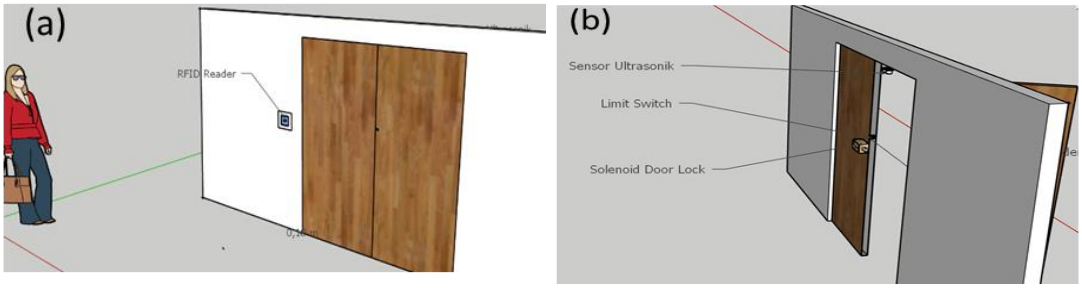

Figure 8. The hardware system from (a). Outside the door and (b). Inside the door

In Figure 8(a) it can be seen that there is a hardware box installed outside the room and there is also an RFID reader to read the RFID tag when the tag is brought near the sensor. Then in Figure 8(b) it can be seen that there are door lock solenoids, limit switches and ultrasonic sensors mounted on the upper door frame. The hardware instrument can be seen in Figure 9. In Figure 9(a) outside the box there are an RC522 RFID reader, buzzer, door lock solenoid, limit switch and ultrasonic sensor. Figure 9(b) inside the box there is a NodeMCU ESP8266 as a processor and relay to disconnect and connect electric current to the door lock solenoid. While the administrative database software can be seen in Figure 10.

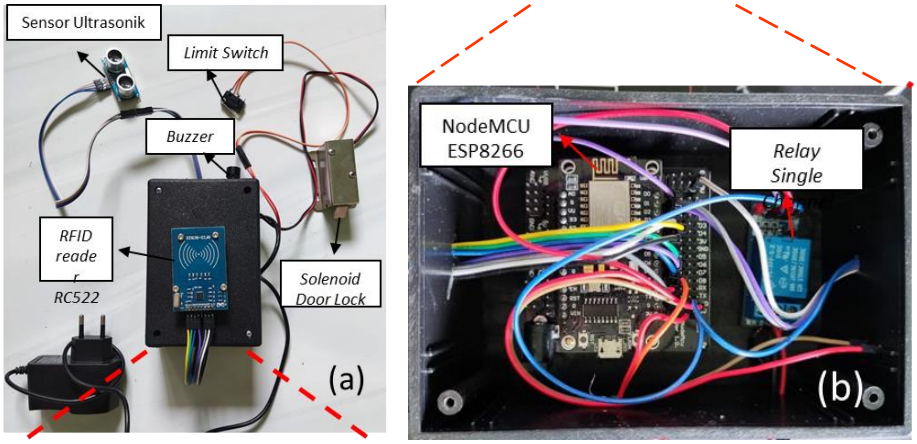

Figure 9. Hardware:(a) outside the box and (b) inside the box

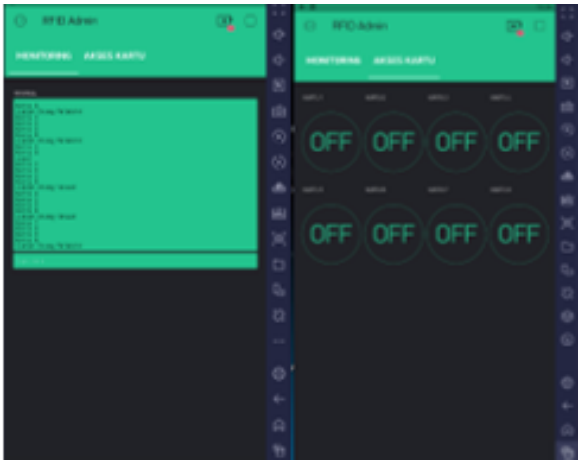

Figure 10. Administrative database software

In the administrative database software, there are 2 menu tabs, namely the monitoring tab to view the cards that are accessing and the card access tab to validate the cards that are allowed and those that are not allowed to be used [17]. When the tag is read by the sensor, in the case that the tag is on the processor memory and has been validated in the administration section, the processor will activate the relay (the relay is in a normally closed state) then the door lock solenoid will unlock the door [16,17]. Then when people pass through the door, it will be detected by ultrasonic sensors and the sensor will count the number of people who pass through the door. If the number of people who pass through the door exceeds 1 person and uses 1 tag, then a violation occurs and turns on the buzzer [18]. After that the door lock solenoid will lock the door again.

3. Results and Discussion

The system is then tested in an actual environment. The first experiment aims to determine the performance of the system against the difference in distance between devices, namely the location of the key system located on the LTJTE door and software devices containing a database for validation. The distance between the two was tested in three conditions namely, 5, 10, and 500 m and the time delay was measured. The time delay is the time lapse between the time the tag is read until the door lock is opened. Trials were carried out on 8 different cards. The test results are shown in Table 1.

Table 1. RFID tag reading delay

Card Name	*Hardware* Location	*Software* Location	Distance (m)	Delay (s)
1	LTJTE	LTJTE	5	2,3
2	LTJTE	LTJTE	5	2,1
3	LTJTE	LTJTE	5	2,5
4	LTJTE	LTJTE	5	1,8
5	LTJTE	LTJTE	5	2,0
6	LTJTE	LTJTE	5	2,3
7	LTJTE	LTJTE	5	3,1
8	LTJTE	LTJTE	5	2,1
1	LTJTE	Building H Lt 2	10	4,2
2	LTJTE	Building H Lt 2	10	4,5
3	LTJTE	Building H Lt 2	10	3,8
4	LTJTE	Building H Lt 2	10	4,0
5	LTJTE	Building H Lt 2	10	4,2
6	LTJTE	Building H Lt 2	10	4,8
7	LTJTE	Building H Lt 2	10	6,1
8	LTJTE	Building H Lt 2	10	5,3
1	LTJTE	Rectorate	500	5,4
2	LTJTE	Rectorate	500	8,7
3	LTJTE	Rectorate	500	6,3
4	LTJTE	Rectorate	500	7,8
5	LTJTE	Rectorate	500	6,2
6	LTJTE	Rectorate	500	5,4
7	LTJTE	Rectorate	500	7,1
8	LTJTE	Rectorate	500	5,8

For more details, the time delay is presented graphically and can be seen in Figure 11.

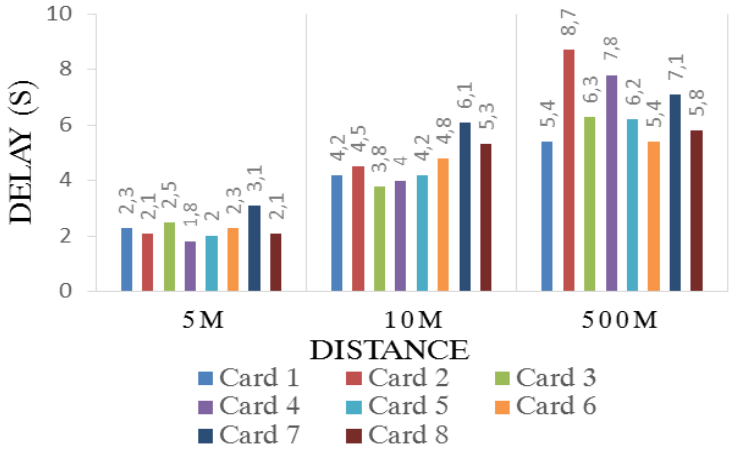

Figure 11. RFID tag reading delay

When the distance between hardware and software devices is 5m, the smallest delay value is 1.8s and the largest delay is 3.1s. The average delay with a distance between devices of 5m is 2.275s. When the distance between devices is 10m, the smallest delay is 3.8s while the largest delay is 6.1s and the average is 4.612s. When the distance between devices is 500 m, the smallest delay is 5.4s while the largest delay is 8.7s and the average is 6.587s. From the data above, it can be seen that the distance between devices affects the amount of delay.

The smallest delay is when the distance between devices is 5m, which is 1.8s and the longest delay is when the distance between devices is 500m, which is 8.7s. In addition to distance, other things that affect are the internet connection and disturbances that interfere with internet signals such as trees and buildings. It can be seen that even if the distance between devices is the same, the delay for different cards in different locations is different. The following is the result for the number of people accessing the door from outside the lab using an RFID tag (Table 2).

Table 2. Description of the number of people who pass through the door

Card Name	Number of People Passing the Door	*Buzzer*	Description
1	1	Off	No violation
2	1	Off	No violation
3	1	Off	No violation
4	1	Off	No violation
5	1	Off	No violation
6	1	Off	No violation
7	1	Off	No violation
8	1	Off	No violation
1	2	On	Violation
2	2	On	Violation
3	2	On	Violation
4	2	On	Violation
5	2	On	Violation
6	2	On	Violation
7	2	On	Violation
8	2	On	Violation

From Table 2 it can be seen that the system has worked as desired. The system is designed to be able to count the number of people who pass through the door according to the RFID tag used, for which only one person through the door for each reading of one RFID tag. From the data, it can be seen that for each RFID tag used, if the number of people who pass through the door is 1 person, then there is no violation, which is indicated by the buzzer off. Meanwhile, if 2 people pass through the door using one card, the system detects a violation which is indicated by the buzzer being on. The system is also highlighted by others [17,18].

e-ISSN: 2722-8363 p-ISSN: 2722-8371

5. Conclusions

Based on the data obtained, it can be seen that the system is realized and can work according to the plan. From the test data, it is found that the distance between devices affects the amount of delay time, where the smallest delay is when the distance between devices is 5m, which is 1.8s and the longest delay is when the distance between devices is 500m, which is 8.7s. In addition to distance, other things that affect are the internet connection and disturbances that interfere with internet signals such as trees and buildings. It is concluded from the fact that even if the distance between devices is the same, the delay among cards is different from one another. In addition, it has been tested that each RFID tag can only be used by one person, otherwise the buzzer will sound indicating that more than one person uses the tag.

Acknowledgments
The author would like to thank those who have contributed to the completion of this research. This research was funded by the University of Lampung through a 2021 FT DIPA research grant.

References

[1] Seneviratne, P. (2015) *Internet of Thing with Arduino Blueprints*, Packt Publishing, Birmingham.

[2] Rerungan, J. (2014) Sistem Pengaman Pintu Otomatis Menggunakan Radio Frequency Identification (RFID) Tag Card Dan Personal Identification Number (PIN) Berbasis Mikrokontroler AVR ATmega 128, *Jurnal MEKTRIK No.1: Universitas Tadulako*, vol. 1, 30-36.

[3] Saputro, E., Wibawanto, H. (2016) Rancang Bangun Pengaman Pintu Otomatis Menggunakan E-KTP Berbasis Mikrokontroler ATmega328, *Jurnal Teknik Elektro No. 1 : Universitas Negeri Semarang*, vol. 8, 98-104.

[4] Winagi, G. F. A., Novianti, T. (2019) Rancang Bangun Pintu Otomatis dengan Menggunakan RFID, *Jurnal Teknik Elektro Dan Komputer Triac : Universitas Bina Sarana Informatika*, vol. 6, 46-50.

[5] Owen, B. (2004) *Dasar- Dasar Elektronika*, Erlangga, Jakarta.

[6] Setiawan, E. B., Kurniawan, B. (2015) Perancangan Sistem Absensi Kehadiran Perkuliahan dengan Menggunakan Radio Frequency Identification (RFID), *Jurnal CoreIT*, Vol. 1, No. 2, 98-105.

[7] Astola, J., Stankovic, R. (2006), *Fundamentals of Switching Theory and Logic Design vol. 5*, Springer, Boston.

[8] Hunt, D., Puglia, A., Puglia, M. (2007) *RFID: A Guide to Radio Frequency Identification*, Wiley, Washington DC.

[9] Ahsan, K., Shah, S., Kingston, P. (2010) RFID Applications: An Introductory and Exploratory Study, International *Journal of Computer Science Issues : Royal College of Surgeons Ireland*, vol. 7, 50-62.

[10] Gustari, R., Fatimah, D. D. S. (2017) Perancangan Sistem Pembaca Kartu Mahasiswa Berbasis Radio Frequency Identification, *Jurnal Algoritma Sekolah Tinggi Teknologi Garut : Sekolah Tinggi Teknologi Garut*. 14, 45-50.

[11] Fauziah, H.Y., Sukowati, A. I., Purwanto, I. (2017) Rancang Bangun Sistem Absensi Mahasiswa Sekolah Tinggi Teknik Cendekia (STTC) Berbasis Radio Frequency Identification (RFID), *Seminar Nasional Sains dan Teknologi*, Jakarta.

[12] Frederic, M. J. (1976) *A systematic Approach to Digital Logic Design*, Addison Wesley, New York.

e-ISSN: 2722-8363 p-ISSN: 2722-8371

[13] Rachmat, H. H., Hutabarat, G. A. (2014) Pemanfaatan Sistem RFID sebagai Pembatas Akses Ruangan, *Jurnal ELKOMIKA: Itenas*, vol. 2, 27-39.

[14] Onibala, J., Lumerta, A. S.M., Sugiarto, B. A. (2015) Perancangan Radio Frequency Identification (RFID) untuk Sistem Absensi Berbasis Mikrokontroler ATmega 8535, *Journal Teknik Elektro dan Komputer*, Vol. 1, No. 7, 45-53.

[15] Yarbrough, J. M. (2012) *Digital Logic: Applications and Design*, Cengage Learning, New Delhi.

[16] Floyd, T. L. (2017) *Digital Fundamentals 11Th Edition, Pearson*, New York.

[17] Neforawati, I., Fareza, M. I., Juniarti, V. (2015) Rancang Bangun Aplikasi Sistem Informasi Monitoring Absensi Mahasiswa Politeknik Jakarta Menggunakan Teknologi NFC pada Android, *Jurnal Politeknologi*, Vol. 14, 2, 19-27

[18] Arief, U. M. (2011) Pengujian Sensor Ultrasonik PING untuk Pengukuran Level Ketinggian, *Jurnal Ilmiah Elektrikal Enjiniring : Universitas Hasanuddin*, vol. 9, 72-77.