ISSN 2347 - 3983
Volume 8. No. 10, October 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter898102020.pdf
https://doi.org/10.30534/ijeter/2020/898102020

Password-Like Scanning Pattern for Enhancing Security Level of RFID-based Door Lock

Heru Supriyono[1], Indra Hermawan[1], Ratnasari Nur Rohmah[1]
[1]Department of Electrical Engineering, Universitas Muhammadiyah Surakarta, Indonesia,
Heru.Supriyono@ums.ac.id, indraey@gmail.com, Ratnasari@ums.ac.id

ABSTRACT

The weakness of using one layer security technique based on Radio Frequency Identification (RFID) for door lock is that the unauthorized person still could unlock the door by using a stolen or cloned RFID card. The objective of this article is to improve the security level of RFID-based door lock by adding one security layer namely RFID card scanning pattern. Research and development method was used in the development and testing process. The proposed system was implemented in the laboratory-scale model with door lock was modeled by using direct current (DC) micro servo. The proposed system equipped with two RFID reader units and a main controller unit. In order to be granted an access or unlock the door, a person should scan the RFID card on the two RFID readers in the correct scanning pattern using a valid RFID card. The scanning pattern is like a password or Personal Identification Number (PIN) commonly used for various applications. The tests results showed that the system was able to recognize the correct pattern and valid RFID card, if the pattern was correct and the card was valid then access was accepted and the door was unlocked for a predetermined time, in the experiment it was 10 seconds, otherwise the access was denied. The experiment also showed that every reader needs at least 0.2 seconds in the range of maximum 3.3 cm to read the RFID reader successfully. The test results suggested that the addition of a password-like scanning pattern able to enhance RFID-based door lock.

Key words : Door lock, multilayer security, RFID based lock, scanning pattern.

1. INTRODUCTION

House or office security is still an important factor for people especially when there are valuable items stored in the house or office. Breaking doors or windows to get in the house or office was commonly practiced by thieves. Mechanical door lock which is using a physical key to be inserted in the key-housing to lock the door is still widely used worldwide. The disadvantage of the mechanical door lock is that the key could be duplicated easily so that unauthorized people could open the door by using this duplicate key.

Nowadays, the usage of electronics technology for home automation is gaining significant attention from researchers such as for home appliances automation [1], for home monitoring [2] and for automating the parking environment of the home [3]. Furthermore, besides for automating home, attempts for improving security of mechanical door lock using electronics technology have also been proposed by researchers for example was by using Android application where the door lock could be locked and unlocked by pressing the button of the Android application then the Android application send the command to the door lock controller using bluetooth data communication [4].

Another technique was proposed by using a secret Personal Identification Number (PIN) where people have to insert a correct PIN by pressing a 4x4 size keypad in order to open the locked door [5]. Similar system architecture but by using alphanumeric keypad component to facilitate password as a key was proposed by researchers in [6]. Another system architecture was using plug-in keypad for extra security means that the keypad for entering PIN or password could be removed from the main door lock systems and bring by the homeowner the same as bringing mechanical key [7]. By using this security technique, a single PIN or password could be assigned for all authorized people or each person could be facilitated to have a unique PIN or password. However, because the PIN or password was implemented in 4x4 keypad which including number from 0-9 plus four alphabet ABCD and four characters the drawback of this technique is that the PIN or password could be known by unauthorized people relatively easily such as by using brute force or other techniques such as social engineering.

Another improvement was reported in [8] and also in [9] where Radio Frequency Identification (RFID) technology was proposed for door lock to replace mechanical door lock. The door could only be opened by authorized people who have a valid RFID card. An RFID card has a tag in it which can be inserted as a unique code. This code should be different from

those of other tags in order to provide an authentication. Other researchers in [10] added a short message services (SMS) based notification warning to RFID-based door lock so that if there was a force break on the door then the system sent a warning message to the homeowner. However, there are some challenges and weaknesses of using RFID cards such as cloning and impersonating [11]. Cloning means an attempt to inject an RFID tag with the same code as the targeted card so that more than one RFID tag has the same code while impersonating means that the people who bring the valid RFID card are not the right person who should bring the card for accessing the door.

In order to improve an RFID based security, researchers proposed a double security system such as using RFID tag plus iris recognition [12] where a person would be granted permission to unlock the door if it provides a valid RFID card and has correct iris. Another improvement was a combination of RFID and face recognition where the door could only be unlocked if the user provided a valid RFID card and the user's face had been stored in the database [13], [14]. Moreover, researchers in [15] proposed combination of RFID and fingerprint as a dual security protection of door lock where the door lock only could be unlocked by a person who has valid RFID card and fingerprint while research results in [16] proposed multilayer security for door lock using RFID card and short message services (SMS) of Global Systems for Mobile (GSM) networks where a person would be able to unlocked and open the door if provide valid RFID card and correct one time password on sent by using GSM networks. Further research result was by combining three security techniques involving RFID, password/PIN by using keypad, and voice recognition [17].

The use of a password-like scanning pattern of RFID cards for door locks has not been reported by researchers yet. The objective of this article is to improve the security level of RFID-based door lock by adding one security layer namely RFID card scanning pattern.

2. MATERIALS AND METHOD

2.1 Authentication Scenario of the Model

The general scenario of the model could be explained as follows. The door of the building or room would be equipped with an electronic system based door lock. Every authorized person would be given an RFID card which has a unique RFID code in it. The data of a valid RFID card would be stored in the database. In order to open the door lock, a person has to provide a valid RFID card and then scan it to the RFID readers of the electronic system based door lock using a certain pattern. If the pattern is correct and the RFID card is valid then the lock would be opened otherwise it would not. In this application, the RFID card was chosen as the main key because it gained more satisfaction for door lock compared to other technologies such as infrared, fingerprint and PIN code [18].

2.2 System Architecture

The proposed model has RFID readers in order to read the pattern of RFID card scanning. As can be seen in Figure 1, as a model, in this article, the model has two RFID readers.

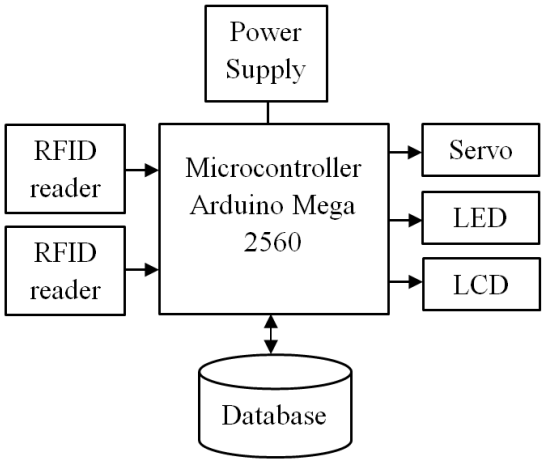

Figure 1: Block Diagram Representing the Proposed System

Every RFID reader will scan the RFID card and then send the data to the Arduino Mega 2560 microcontroller as the main processor. Microcontroller was preferred to be used as the main controller over other instruments because it has small size, low power consumption and reliable so that it has been widely used by researchers such as for developing a wheeled robot for detecting gas leakage [19] and a portable environment monitoring system [20]. The microcontroller then checks both the scanning pattern and the validity of the RFID card and compares it to the data stored in the database. If both parameters are correct then the microcontroller sends commands to activate a direct current (DC) micro servo as door lock model, to turn on green Light Emitting Diode (LED) as indicator, and to display permission message on a Liquid Crystal Display (LCD). As a contrast, if there is either incorrect pattern or invalid RFID card then the microcontroller sends commands to turn on the red LED and to display a denial message on the LCD. The DC micro servo is able to rotate 180 degrees to model the door lock in the position of unlocked and locked.

In this article, off the shelf RFID cards which are available commercially (shown in Figure 2) were used in the development and experimental phase. The card has memory for storing information including a unique code and an antenna for transmitting the data in wireless using electromagnetic waves. The card has a passive type RFID tag in it which uses 125 KHz electromagnetic waves for

transmitting the data. In the passive type RFID tag, the tag will wait and responsd to the signal transmitted by the RFID reader. So that, both RFID card and reader have to use the same frequency of electronic wave in order to communicate successfully.

Figure 2: The Physical Appearance of RFID Card Used in the Experiment

Arduino Mega 2560 Microcontroller (shown in Figure 3) is a development board which has 54 inputs/outputs (I/O)s digital pins (15 of them are a Pulse Width Modulation (PWM)), 16 analogue input pins, and 4 serial port hardware or UART pins. It has 16 MHz oscillator, one Universal Serial Bus (USB) port, direct current (DC) power input, and reset button. Arduino Mega 2560 is a popular microcontroller and used in many applications [21].

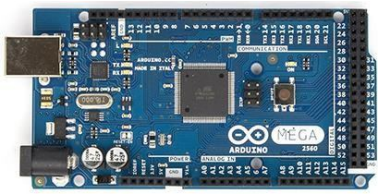

Figure 3: Physical Appearance of Arduino Mega 2560 Board

The LCD used in the experiment is a 16 x 2 LCD type means that it has 16 columns and two rows to display the information. It has 16 pins in total but only 10 pins used namely VDD, VSS, VEE, D7, D6, D5, D4, RW, RS, and E. The connection between Arduino Mega 2560 and the LCD is as follows: pin RW is connected to GND, RS is connected to pin 12, E is connected to pin 11, D7 is connected to pin 2, D6 is connected to pin 3, D5 is connected to pin 4, D4 is connected to pin 5 as outlined in the schematic diagram of Figure 4.

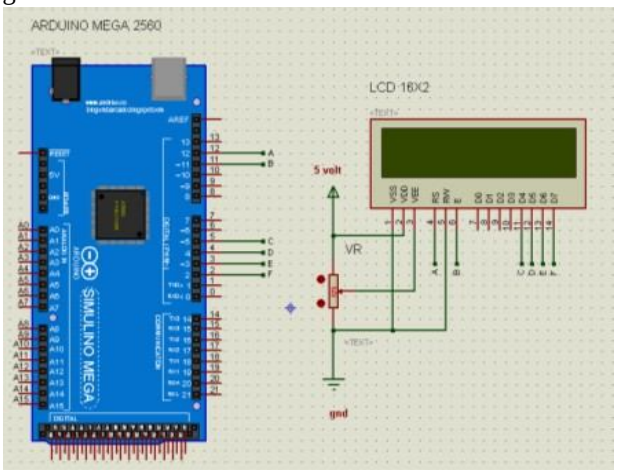

Figure 4: Schematic Diagram for Connecting Arduino Mega 2560 Microcontroller Board and LCD

2.3 Software Design

The main software is the software developed for the microcontroller. Firstly, after starting or initialization process, the microcontroller reads the data of every RFID reader. If the RFID reader is ready to use then it turns on the LED indicator and the microcontroller sends a command to display that RFID reader is active and ready to display RFID code. Secondly, the microcontroller will check the pattern of the RFID card scanning. Because there are two RFID readers, in order to be recognized easier, the RFID reader is marked as RFID reader A (RA) and RFID reader B (RB). In this article, as a concept of proof, the correct pattern scanning was determined as RA-RB-RA-RA. So that, for the first instance, the microcontroller will check whether there is an RFID card scanned in RA if yes then it will continue to RB and so on. If not, for example the RFID reader is scanned to the RB in the first instance, then the microcontroller will generate a command to end the routine and does not give any response. If the pattern is correct, then the last process is the checking whether the RFID card is valid or not. If the RFID card is valid then the microcontroller will generate a command for turning on the green LED, displaying permission message on LCD and turning on the servo otherwise it turning on red LED and displaying denial message on LCD. The overall computation process is presented on the flowchart in Figure 5.

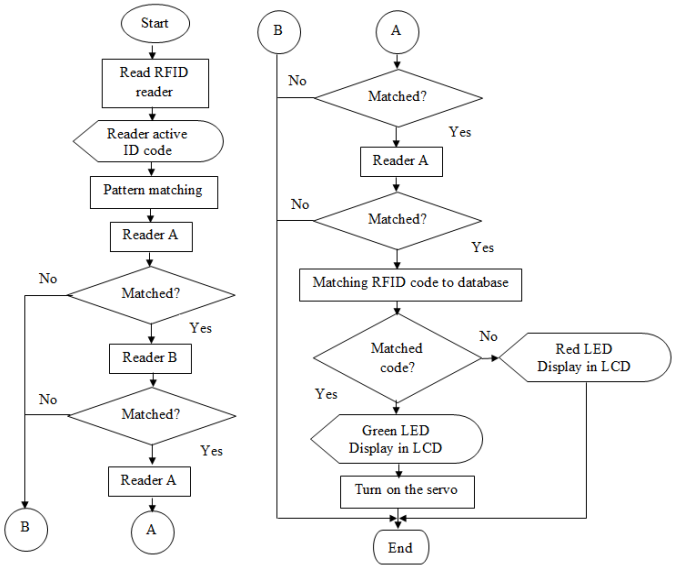

Figure 5: Flowchart Representing Overall Computation Process of the System

3. RESULTS AND DISCUSSION

3.1 Actual System Obtained

In order to protect them, all hardware components of the proposed system were placed in three plastic boxes, i.e. one box for the main controller unit and two boxes for RFID readers units. The main controller box has an LCD display on

its surface as can be seen in Figure 6. Two boxes of reader units containing RFID reader circuits are depicted in Figure 7. Each box has an LED indicator on its surface. The LED will be turned on in blue light if the reader is in standby condition, green light if the RFID card is valid or access is accepted and red light if the RFID card is invalid or access is denied.

Figure 6: The Main Controller Unit Box

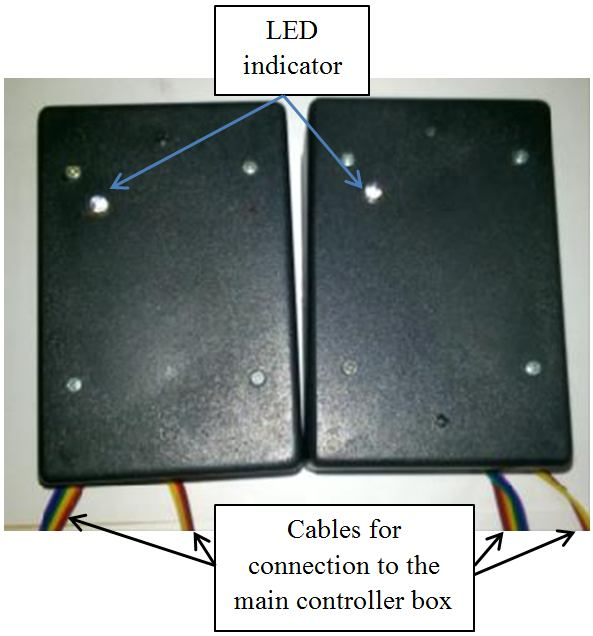

Figure 7: Two Reader Unit Boxes Containing RFID Reader Hardware Circuits

Steps of systems usage could be explained as follows. First, the system has to be turned on by connecting it to the power source until it is in the active condition. The active condition of the RFID scanner box is indicated by the blue LED turned on shown in Figure 8 while the active condition of the main controller unit is indicated by the LCD displaying a message to scan the RFID card as can be seen in Figure 9. After the system is in the standby condition then users would be able to scan the RFID card. If the RFID reader is able to read the RFID card then it turns on the green LED and the controller box displaying a message showing which reader is being used for scanning the RFID card and its corresponding code as depicted in Figure 10 and 11. On the contrary, if the RFID reader is unable to read the RFID card then it turns on the red LED as depicted in Figure 12 and then the whole system back to the standby condition.

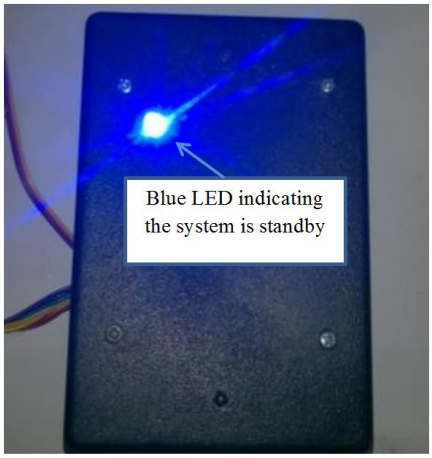

Figure 8: Blue LED of the Reader Box Indicating that the System is in Standby Condition

Figure 9: The System is in Active or Standby Condition if the LCD of the Controller Displays a Message "Please scan the card' (the interface uses *Bahasa Indonesia*).

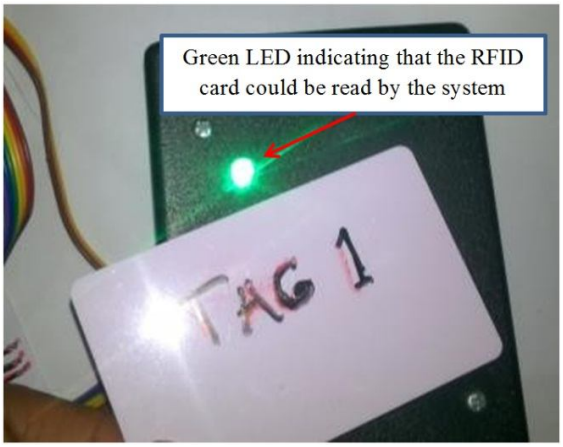

Figure 10: Green LED of the Reader Box Indicating that the Reader Able to Read the RFID Card

Figure 11: LCD of the Controller Box Displas RFID Code of the Card Being Scanned

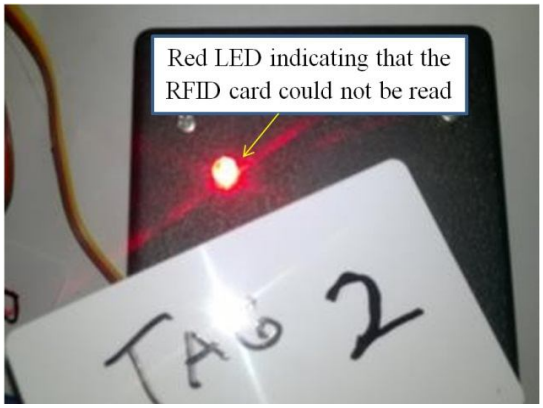

Figure 12: The red LED of the RFID Reader Box is on Indicating that it is Unable to Read the RFID Card

3.2 RFID card reading test

The RFID card reading test was carried out by scanning all RFID cards used in the experiment to the RFID readers of the system namely Reader A and Reader B. Every card has a tag inside of it which has unique code. If the RFID card is successfully read by the reader then the LCD of the controller box displays which reader is used for reading the RFID card and what is the unique code of the corresponding RFID tag being scanned. There are four RFID cards used in the experiment. Every RFID card was scanned five times consecutively. The test results presented in Table 1 shows that all readers were able to read the RFID card and the LCD of the controller able to display its corresponding code consistently.

Table 1: RFID card reading test results

Reader	Tag	Status	LED	Display in LCD
A	1	Success	Green	Reader A: A34F21ED
B	1	Success	Green	Reader B: A34F21ED
A	2	Success	Green	Reader A: E9EF4F35
B	2	Success	Green	Reader B: E9EF4F35
A	3	Success	Green	Reader A: 1939ECD5
B	3	Success	Green	Reader B: 1939ECD5
A	4	Success	Green	Reader A: A29FB4D5
B	4	Success	Green	Reader B: A29FB4D5

3.3 RFID card reading test for various distance

This test was performed to confirm the optimal distance of the RFID card from the reader box in the scanning process. Test was done by scanning the RFID card at a certain distance from the reader. There were a minimum five scanning attempts performed for every distance. The test results presented in Table 2 showed that the reader would be able to read the RFID card in the distance maximum of 3.3. cm. If the distance is more than 3.3 cm then the reader could not read the RFID any more.

Table 2: Reading testing results for various distance between RFID reader and tag

Tag	Distance (cm)	Results	
		Reader A	Reader B
1	1	Success	Success
1	2	Success	Success
1	2.5	Success	Success
1	3	Success	Success
1	3.3	Success	Success
1	3.5	Fail	Fail
1	4	Fail	Fail

3.4 Scanning time test

Scanning time test was done to unveil the minimum time needed by the reader to read the RFID card. The test was performed by scanning the RFID card on RFID readers in a certain determined time. The determined scanning time was measured by using an electronics stopwatch. Whether the reader was able to read the RFID card or not would be indicated by the color of the LED in the reader box, if the green LED was turned on then the reader was able to read the RFID card otherwise the red LED was turned on. If the reader was able to read the RFID reader then the LCD of the controller box displayed the corresponding RFID code. The results in Table 3 shows that every reader needs 0.2 seconds in minimum for scanning the RFID card. If the scanning time is less than 0.2 second then the reader would not be able to read the RFID card even if the RFID card is valid.

Table 3: Reading test results for various given reading time

Tag	Reader	Time (s)	Status	Display in LCD
1	A	0.1	Fail	None
1	B	0.1	Fail	None
1	A	0.2	Success	A34F21ED
1	B	0.2	Success	A34F21ED
1	A-B	0.4	Success	A34F21ED
1	A-B-A	0.8	Success	A34F21ED
1	A-B-A-A	1.2	Success	A34F21ED
1	A-B-A-A-B	1.5	Success	A34F21ED

3.5 Scan with correct pattern and validity test

In order to test whether the system able to recognize both correct pattern and valid RFID code, the test was performed by scanning valid RFID card with correct pattern, i.e. RA-RB-RA-RA and scanning invalid RFID cards with the correct pattern. The test results presented in Table 4 shows that when both reading pattern is correct and the RFID code is valid (test number 1-4) then the access is accepted indicated by LCD of the controller box displays message "You are permitted Welcome" as depicted in the Figure 13 and the microcontroller of the controller cox turns on servo motor as action model for opening the door for certain predetermined time which in this publication is equal to ten seconds. However, although the scan pattern is correct but the RFID code is not matched to the database (test number 5), the access would be denied and the LCD of the controller box will display a message "You are not permitted to come in" as depicted in figure 14.

Table 4: Reading test results with correct pattern

Tag	Reader		Pattern	Status
	A	B		
1	Success	Success	RA-RB-RA-RA	Accepted
2	Success	Success	RA-RB-RA-RA	Accepted
3	Success	Success	RA-RB-RA-RA	Accepted
4	Success	Success	RA-RB-RA-RA	Accepted
5	Success	Success	RA-RB-RA-RA	Denied

Figure 13: Message Displayed by the LCD When the Access is Accepted

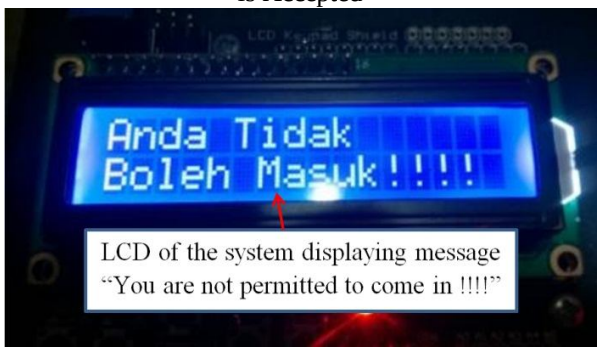

Figure 14: Message Displayed by the LCD When the Access is Denied

3.6 Scan with incorrect pattern test

The test was carried out for confirming whether the system able to recognize the incorrect pattern. There were five RFID cards used in the experiment including four valid cards and one invalid card. For every RFID card, there were five consecutive incorrect pattern attempts test. The test results in Table 5 shows that the system was able to detect the incorrect pattern and deny the access both for valid and invalid RFID cards.

Table 5: Reading test results with incorrect pattern

Tag	Reader		Pattern	Status
	A	B		
1	Success	Success	RA-RA-RB-RA	Denied
2	Success	Success	RB-RB-RB-RA	Denied
3	Success	Success	RA-RB-RB-RA	Denied
4	Success	Success	RA-RB-RA-RB	Denied
5	Success	Success	RA-RB-RB-RB	Denied

3.7 Discussion

The comparison of proposed system to password or PIN based door lock systems is presented in Table 6. It can be noted that compared to other PIN/password systems, the proposed system has secondary security techniques, i.e. the validity checking of RFID code. The system proposed in [7] also has secondary security means in the form of that the 4x4 keypad circuit could be unplugged and brung by the user. However, this technique is less praticable since bringing the 4x4 keypad circuit is not as simple as bringing an RFID card. Also, SMS warning notification needs extra cost to maintain the balance of GSM networks.

Table 7 shows the comparison of the proposed system to other RFID-based door lock systems is discussed as follows. The door lock system which uses RFID technique only highly depending on the RFID code. If the RFID card is stolen or being cloned, then there is no secondary protection. In contrast, the proposed system offers a second protection by using a password-like reading pattern of RFID card means that if a person bring a stolen or cloned RFID card he/she still needs to provide the correct scanning pattern in order to unlock the door. Compared to research result in [10], the proposed system does not need extra recurring cost for GSM networks maintenance.

Compared to other multi-layer RFID security techniques as presented in Table 8, it can be noted that the proposed system is different from research published by other researchers. The proposed system is considerably simpler and cheaper because it only used one microcontroller as main controller compared to research results in [12], [13], [14] which computer or computer plus microcontroller. So that, in our view, the

proposed system is more practicable for home or room application than those systems. Moreover, compared to research results in [16] the proposed system is simpler and cheaper because it does not need extra cost for GSM maintenance.

Table 6: Comparison of proposed system to other PIN/password based systems

Aspect	Proposed System	System in [5]	System in [6]	System in [7]
The first layer security technique	RFID code Password-like scanning pattern of RFID card	PIN	Password	Password
The second layer security technique	RFID code	-	-	Unplugged keypad
Additional security feature	Red LED alert	Buzzer	-	Buzzer, SMS warning notification

Table 7: The comparison of proposed system to other RFID-based door lock systems

Aspect	Proposed System	System in [8]	System in [9]	System in [10]
The first layer security technique	RFID code Password-like scanning pattern of RFID card	RFID code	RFID code	RFID code
The second layer security technique	RFID code	-	-	-
Additional security feature	Red LED alert	-	Buzzer alert	GSM-based SMS warning notification

Table 8: The comparison of proposed system to other RFID-based multilayer door lock systems

Aspect	The Proposed System	System in [12]	System in [13]	System in [14]	System in [15]	System in [16]	System in [17]
The first layer security	RFID code Password-like scanning pattern of RFID card	RFID code	RFID code	RFID code	RFID code	RFID code	RFID code
The second layer security	RFID code	Iris recognition	Face recognition	Face recognition	Finger-print	One time password using 4x4 keypad	Voice recognition
The third layer security	-	-	-	-	-	-	Password/PIN using 4x4 keypad
Additional security feature	Red LED alert	-	-	GSM based emergency call, alarm	-	Buzzer	-

5. CONCLUSION

Based on the design and testing results it could be concluded that the model of the password like pattern reading of RFID card for door lock has been successfully developed. The proposed system is equipped with two RFID readers and one main controller circuit. The tests results showed that the system was able to recognize the correct pattern and valid RFID card in order for opening the door lock, if both patterns were correct and the card was valid then access was accepted and the door lock was opened for certain predetermined time otherwise the access was denied. These results suggested the addition of password-like scanning patterns able to enhance the security level of RFID-based door locks. The experiment also showed that every reader needs at least 0.2 seconds in the maximum range of 3.3 cm to read the RFID reader successfully. However, the proposed system was still in the form of a model, it has not been developed in real size and condition which can be addressed in the future work.

REFERENCES

1. S. Ghanghas, S. Dahiya, M. K. Pandey, S. Tripathi. **Design and Development of IoT based Intelligent Home Automation System**, *International Journal of Emerging Trends in Engineering Research (IJETER)*, vol. 8, no. 7, pp. 3487-3494, July 2020.

2. M. R. Kumar, and R. H. Sree. **Home Computerization Monitoring System with Google Supporter**, *International Journal of Emerging Trends in Engineering Research (IJETER)*, vol. 8, no. 6, pp. 2240-2244, June 2020.
3. Anchal, and P. Mittal. **IoT Based Intelligent Modeling of Smart Home Parking Environment**, *International Journal of Emerging Trends in Engineering Research (IJETER)*, vol. 8. no. 7, pp. 3442-3446, July 2020.
4. N. H. Ismail, Z. Tukiran, N. N. Shamsuddin, and E. I. S. Saadon. **Android-based Home Door Locks Application via Bluetooth for Disabled People**, *in Proceedings of 2014 IEEE International Conference on Control System, Computing and Engineering*, pp. 191-195 28 - 30 November 2014.
5. E. Z. Orji, U. I. Nduanya, and C. V. Oleka. **Microcontroller Based Digital Door Lock Security System Using Keypad**, *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, vol., no. I, pp. 92-97, January 2019.
6. A. Jain, A. Shukla, and R. Rajan. **Password Protected Home Automation System with Automatic Door Lock**, *MIT International Journal of Electrical and Instrumentation Engineering*, vol. 6, no. 1, pp. 28-31, January 2016.
7. A. D. Odu, M. C. Alice, and O. J. Odinya. **Low Cost Removable (Plug-In) Electronic Password - Based Door Lock,** *American Journal of Engineering Research (AJER)*, vol. 6, no. 7, pp-146-151, 2017.
8. G. K. Verma, and P. Tripathi. **A Digital Security System with Door Lock System Using RFID Technology**, *International Journal of Computer Applications (0975 – 8887)*, vo. 5, no.11, pp. 6-8, August 2010.
9. N. Asha, A. S. S. Navaz, J. Jayashree, and J. Vijayashree. **RFID Based Automated Gate Security System**, *ARPN Journal of Engineering and Applied Sciences*, vol. 13, no. 22, pp. 8901-8906, November 2018.
10. H. Deviana, M. M. Amin, R. Sandy, P. T. Nguyen, W. Hashim, A. Maseleno. **Door Security Design using Radio Frequency Identification With a Short Message Service Warning System**, *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2S2, pp. 354-370, July 2019.
11. M. El Beqqal, and M. Azizi. **Review on security issues in RFID systems**, *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 6, pp. 194-202, 2017.
12. P. P. Chitte, G. J. Rana, and S. Taware. **Advanced Security System using RFID and IRIS Recognition System using ICA, PCA, Daugman's Rubber Sheet Model Together**, *International Journal of Computer Applications*, vol. 48, no.13, pp. 5-11, June 2012.
13. A. Affandi, M. Awedh, M. Husain, and A. Alghamdi. **RFID and Face Recognition Based Security and Access Control System**, *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 2, no. 11, pp. 5955-5964, November 2013.
14. U. Farooq, M. U. Hasan, M. Amar, A. Hanif, and M. U. Asad. **RFID Based Security and Access Control System**, *International Journal of Engineering and Technology*, vol. 6, no. 4, pp. 309-314, August 2014.
15. M. M. R. Komol, A. K. Podder, M. N. Ali, and S. M. Ansary. **RFID and Finger Print Based Dual Security System: A Robust Secured Control to Access Through Door Lock Operation**, *American Journal of Embedded Systems and Applications*, vol. 6, no. 1, pp. 15-22, 2018.
16. K. Deka, R. J. Gogoi, S. Jhavar, and H. Gogoi. **Design a RFID Technology based Door Security System using GSM Module**, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 6, no. 7, pp. 5862-5868, July 2017.
17. I. Mailabari, K. S. Awuna, and A. M. Kida. 2018. **Design and Implementation of a Microcontroller Based Three Tier Security Lock System**, *International Journal of New Technology and Research (IJNTR)*, vol. 4, no. 6, pp. 98-103, June 2018.
18. M. Anshar, and N. Anas. **Hardware and User Perspective Assessment on Application of Smart Door Access**, *IOP Conf. Series: Materials Science and Engineering*, vol. 676 (2019) 012003, pp. 1-6, 2019.
19. H. Supriyono, and A. N. Hadi. **Designing a wheeled robot model for flammable gas leakage tracking**, in *Proceedings of the second International Conference on Informatics and Computing*, Jayapura, 2017, pp. 1-6, 2017.
20. H. Supriyono, E. D. Febriyanto, and K. Harismah. **Portable Machine to Machine System for Monitoring Temperature and Flammable Gas of Outdoor Environment**, *in AIP Conference Proceedings 2114*, vol. 040014 (2019), pp. 040014-1 - 040014-8, 2019.
21. K. Tshomo, K. Tshering, D. Gyeltshen, J. Yeshi, and K. Muramatsu. **Dual Door Lock System Using Radio-Frequency Identification and Fingerprint Recognition**, *in 2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, 1-6, 2019.