Home Energy Security Prototype using Microcontroller Based on Fingerprint Sensor

Alrizal Akbar Nusantar[1], Ilham Ari Elbaith Zaeni[1], Dyah Lestari[1]

Authors

[1]Department of Electrical Engineering Universitas Negeri Malang, Indonesia.

Corresponding: alrizal.a.n@gmail.com

Abstract

The globalization era brings rapid development in technology. The human need for speed and easiness pushed them to innovate, such as in the security field. Initially, the security system was conducted manually and impractical compared to nowadays system. A security technology that is developed was biometric application, particularly fingerprint. Fingerprint-based security became a reliable enough system because of its accuracy level, safe, secure, and comfortable to be used as housing security system identification. This research aimed to develop a security system based on fingerprint biometric taken from previous researches by optimizing and upgrading the previous weaknesses. This security system could be a solution to a robbery that used Arduino UNO Atmega328P CH340 R3 Board Micro USB port. The inputs were fingerprint sensor, 4x5 keypad, and magnetic sensor, whereas the outputs were 12 V solenoid, 16x2 LCD, GSM SIM800L module, LED, and buzzer. The advantage of this security system was its ability to give a danger sign in the form of noise when the system detected the wrong fingerprint or when it detects a forced opening. The system would call the homeowner then. Other than that, this system notified the homeowner of all of the activities through SMS so that it can be used as a long-distance observation. This system was completed with a push button to open the door from the inside. The maximum fingerprints that could be stored were four users and one admin. The admin's job was to add/delete fingerprints, replace the home owner's phone number, and change the system's PIN. The results showed that the fingerprint sensor read the prints in a relatively fast time of 1.136 seconds. The average duration that was needed to send an SMS was 69 seconds while through call was 3.2 seconds.

Keywords
transformer age, linear trend, load growth, ambient temperature

1. Introduction

Globalisation era brings a rapid development in technology. The human need for speed and easiness pushed them to innovate, such as in the security field. Initially, the security system was conducted manually and impractical compared to nowadays system. Examples of manual security systems were key and padlock; then, with the change of time, it changed into modern systems such as PIN and password. This occurrence proves that the security system experienced a fast development [1]–[6]. A security technology that is developed was biometric application, particularly fingerprint. Biometric system is a self-identification system using body parts or human behaviour. Biometric has the advantages of challenging to forget, difficult to lose, cannot be used at the same time, and hard to duplicate. These advantages cause biometric to be used in automatic self-identification and verification [7]–[12]. There are six general biometrics: fingerprint, iris, face, voice, hand geometry, and signature. The utilisation of biometric is wide, particularly in the areas that require more safety.

Generally, the biometric application is grouped into (1) commercial application, (2) governmental application, and (3) forensic application. Some examples for commercial applications are computer login process (standalone or network), electronic data security system, attendance system, eCommerce, e-banking, internet access, ATM, credit card, access control to the physical facility, cellphone, PDA, medical record, long-distance education, and others. In government application, the examples are ID making, driver's license making, border surveillance, passport making, and others. Meanwhile, the forensic application's examples are criminal investigation, corpse identification, terrorist identification, and determining family relations (DNA). The most used biometric is fingerprint. A fingerprint is a skin that thickens and thins forming a "mountain" on the palm of a finger that forms a pattern [13]–[19]. The fingerprint will not disappear until one dies and rots. Scratches or wounds usually would form the same pattern during skin replacement; however, fingerprint can get damaged due to severe burns.

Fingerprint becomes the most used biometric due to its high accuracy and easy to be applied. The characteristics of a fingerprint are (1) perennial nature, (2) immutability, and (3) individuality. Perennial nature or scratches on fingerprints attached to human skin for life. Immutability is the unchanged fingerprint, unless due to severe accident. Meanwhile, individuality means that each fingerprint is unique, and each person has different fingerprint. Fingerprint-based security became a reliable enough system because of its accuracy level, safe, secure, and comfortable to be used as housing security system identification. Therefore, applying this into a security system could be a useful breakthrough for the community.

This research aimed to develop a security system based on fingerprint biometric taken from previous researches by optimising and upgrading the previous weaknesses. The upgrade was such as the usage of 4x5 keypad to facilitate utilisation and a shortcut for orders. Besides, this system could give a danger sign in the form of noise when the system detects the wrong fingerprint or when it detects a forced opening. The system would call the homeowner then. Other than that, this system notified the homeowner all of the activities through SMS so that it can be used as a long-distance observation.

2. Method

System requirement analysis defined the specific system requirements such as (1) determining the device's body, (2) determining the features, (3) maximum fingerprints for effectivity, (4) fingerprint enrolment process, and (5) fingerprint verification process [14], [16], [20]–[23]. The device was designed in a square shape to make it easier to be put in a horizontal surface. The sensor and actuator were connected to the Arduino Uno board and used jumper cable in the required length.

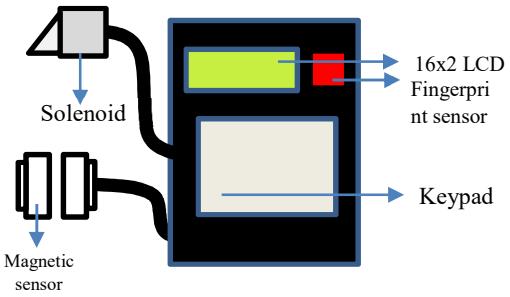


Fig. 1. 2D Device Model

Fig. 2. 3D Device Model

Software design explained how the overall system works through PIN initialisation process, new fingerprint enrolment process, and overall performance process. PIN initialisation process with 4x5 keypad input followed the below flowchart. This process was aimed at the administrator. This process first required PIN input, and to prevent the PIN insertion error, the administrator should enter the PIN once more. After verification, the next step was on the LCD to display the 'PIN verified" text. If the PIN were different from the initial one, the process would be back to the beginning: entering the initial PIN. Backup security works if there is a forced entry that bypassing the fingerprint scanning process — this backup security utilised magnetic sensor. If the sensor identified no scanning process and idle solenoid but the door was opened (active magnetic sensor), the buzzer would go off, and GSM SIM800L module would call the homeowner. With this backup security, the homeowner would know if there is a forced entry. The push-button works to open the door from the inside. Both user and administrator could use this feature. When the solenoid is inactive, and the door is closed, they only need to push the button then the solenoid will become active and open the door for 5 seconds. After 5 seconds, the solenoid will be back to its original position.

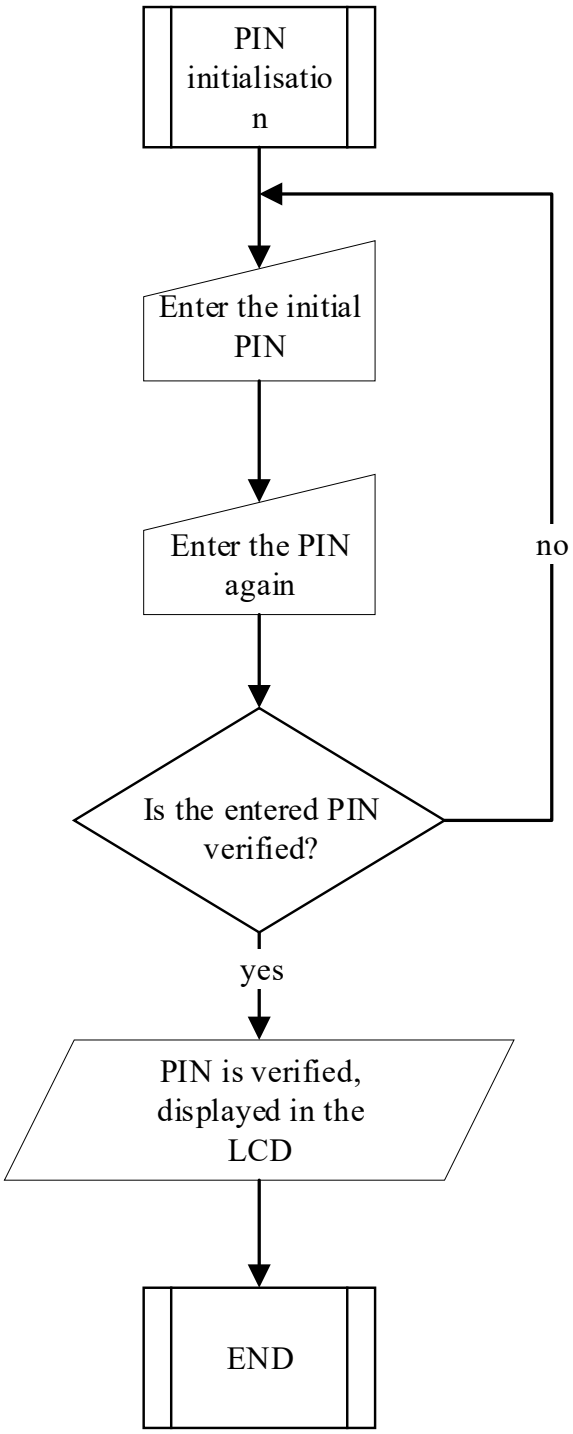


Fig. 3. PIN Initialisation Performance Flowchart

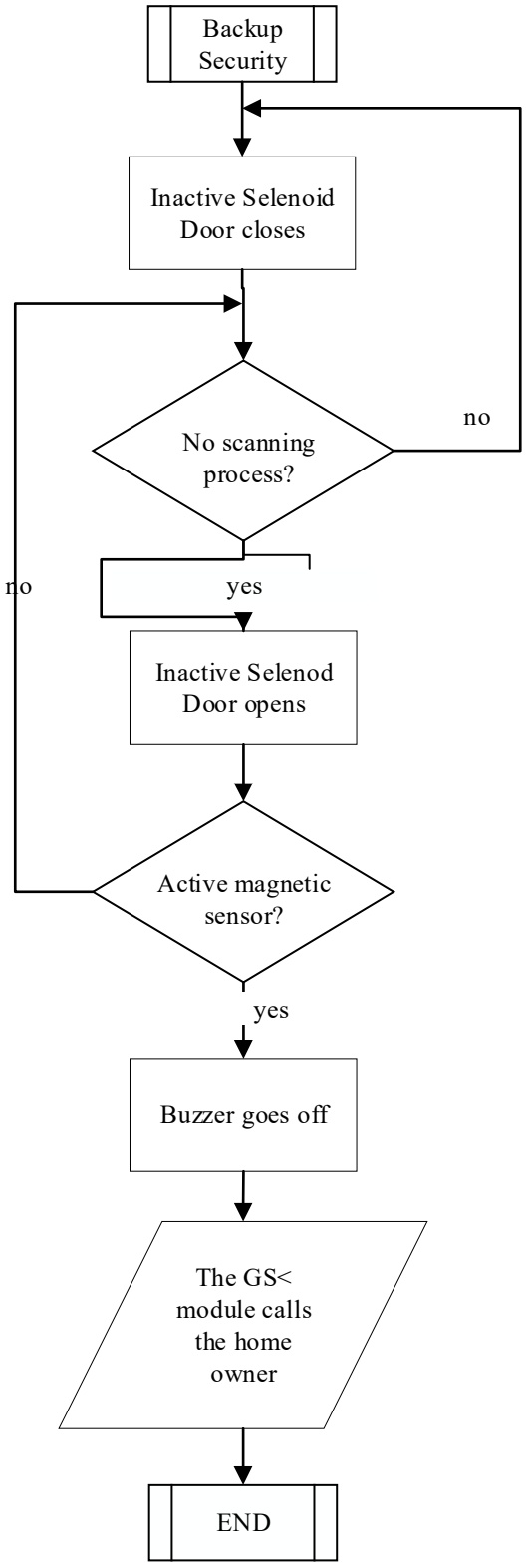


Fig. 4. Backup Security Performance Flowchart

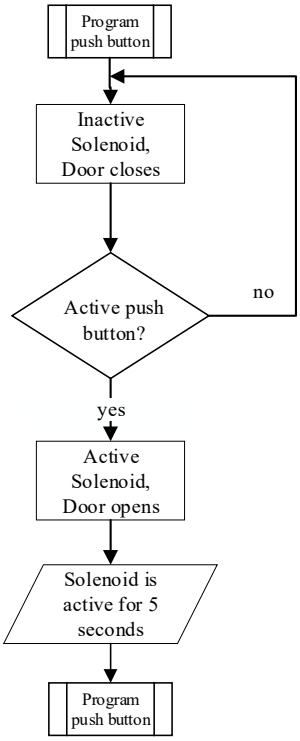


Fig. 5. Push Button Program Flowchart

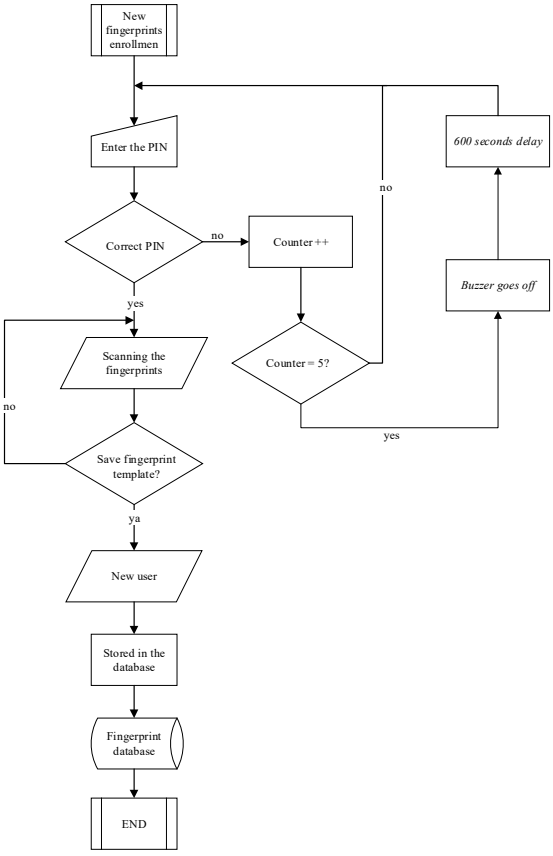


Fig. 6. Fingerprint Enrolment Performance Flowchart

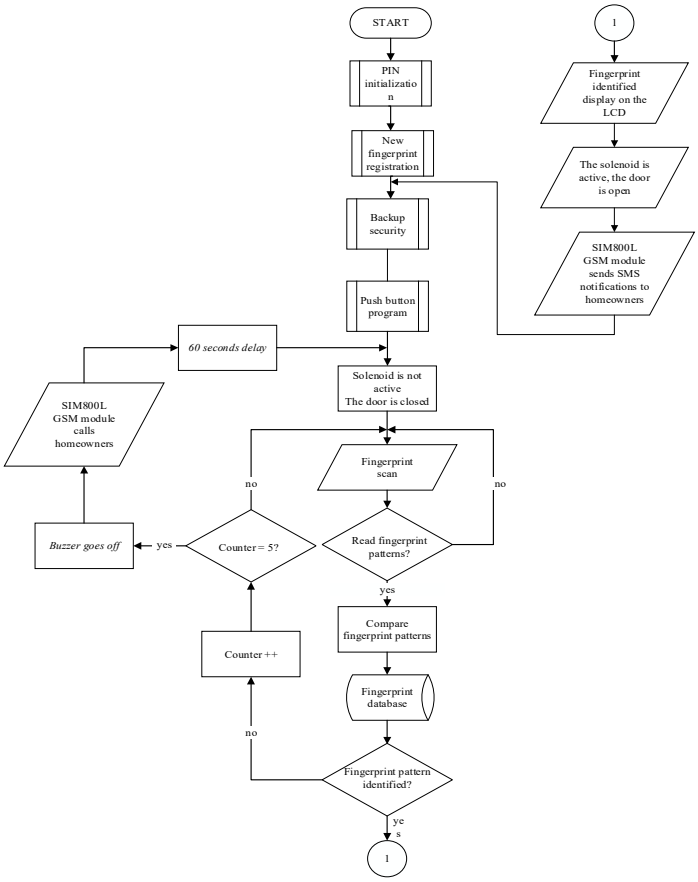


Fig. 7. Overall Performance Flowchart (*Administrator*)

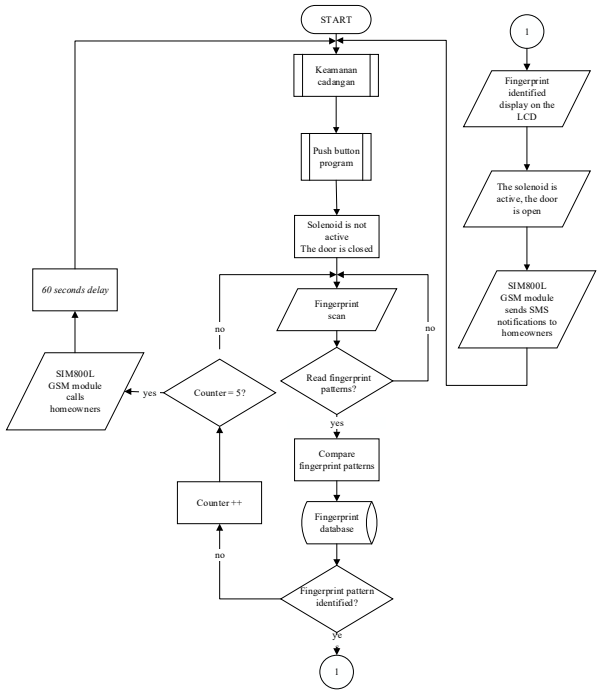


Fig. 8. Overall Performance Flowchart (*User*)

The administrator could only do this process. The first step was entering the set PIN, then scanning the fingerprint. However, a mistake in PIN insertion for five times would result in the GSM SIM800L module to call the homeowner and admin could not use the device for 600 seconds. After fingerprints were saved, they would be saved into a new user in the database. If not, the scanning process was repeated. This is the overall process. The first process was PIN initialisation then fingerprint scanning. PIN initialisation automatically activating the backup security. The next step was the fingerprint scanning process. The sensor would read the fingerprint, then moved to the next step. When the sensor was unable to read the fingerprint, the scanning process would be repeated. Then, the fingerprint would be compared with the data in the database. If identified, then moved to the next step. If not, then back to the fingerprint scanning. After five mistakes in scanning, the SIM800L module would call the homeowner, and the device was unable to be used for 600 seconds. However, after, it still can be used to scan the fingerprints. The identified fingerprint would result in the 'fingerprint identified' text on the LCD. Then, the SIM800L module would notify the homeowner and activating the solenoid to open the house. After all, the process was finished; it would loop again and inactivated the solenoid and close the door.

3. Result

This stage describes the obtained data from the fingerprint sensor test. This stage also analysed and calculated the error percentage from the reading data. The results are shown in the table below.

TABLE 1 FINGERPRINT READING TEST RESULTS

No.	Scanned Finger	User address (ID)	Test (s)					Average (s)
			1	2	3	4	5	
1.	IJN	1	1.2	1.3	1.3	1.1	1.3	1.24
2.	IJR	6	1	1.4	1.3	1.3	1.2	1.24
3.	TN	2	1.2	1.4	1.5	1.2	1.3	1.32
4.	TR	7	1.4	1.2	1.1	1.3	0.8	1.16
5.	HN	3	1.2	1.3	1.3	1.1	1.3	1.24
6.	HR	8	1.1	1.1	1.2	1.2	0.9	1.1
7.	MN	4	1.4	1.9	2.2	1.3	1.5	1.66
8.	MR	9	0.9	1.2	1.4	1.3	0.9	1.14
9.	KN	5	1.3	1.5	1.7	1.5	1.5	1.5
10.	KR	10	1.5	1.3	1.5	2.1	1.8	1.64
Total average (s)								1.324

This test's goal was to find the accuracy of the reading and the duration needed for the sensor in reading the enrolled fingerprints. From the obtained data, all prints were able to be read, and the fastest average duration to read a fingerprint was 1.1 seconds in the left middle finger. The most extended average duration to read a fingerprint was 1.66 seconds in the right ring finger. From the total ten samples, the total average duration was 1.324 seconds. Alternatively, in other words, the sensor could read a fingerprint in an accurate and fast way of 1 second. In this test, the active sensor had 0 V voltage, and inactive sensor had close to 5 V voltage. The tested distance was started from 0 cm up to infinity. Infinity distance is a distance where the magnet is not in a close distance with the switch. The results showed that the magnetic sensor worked from a distance of 0–0.7 cm. Above 0.8 cm, the sensor was unable to work. This occurrence proved that the sensor worked following the database. This magnetic sensor was Normally Open type, meaning that when the magnet clings, the switch closes and vice versa. The distance followed the datasheet with the activated gap below 8 mm (0.8 cm).

TABLE 4 MAGNETIC SENSOR TEST RESULTS

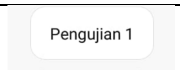
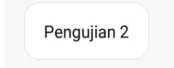
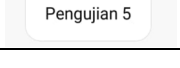
No.	Distance (cm)	Voltage (V)	Magnetic Sensor Condition
1.	0	0	ON
2.	0.1	0	ON
3.	0.2	0	ON
4.	0.3	0	ON
5.	0.4	0	ON
6.	0.5	0	ON
7.	0.6	0	ON
8.	0.7	0	ON
9.	0.8	4.67	OFF
10.	0.9	4.74	OFF
11.	1	4.89	OFF
12.	∞	4.90	OFF

TABLE 5 SOLENOID TEST RESULTS

No.	Input Voltage		Solenoid Voltage (V)	Condition	Explanation
	V_{OL}	V_{OH}			
1.	0.8		3.3	OFF	Inactive solenoid
2.			5	OFF	Inactive solenoid
3.			9	OFF	Inactive solenoid
4.			12	OFF	Inactive solenoid
5.		4.2	3.3	OFF	Inactive solenoid
6.			5	OFF	Inactive solenoid
7.			9	ON	Active solenoid
8.			12	ON	Active solenoid

The solenoid test used random solenoid voltage (V) such as 3.3 V, 5 V, 9 V, and 2 V. the input voltage was LOW voltage (V_{OL}) and HIGH (V_{OH}) microcontroller. The 0.8 V voltage was a LOW microcontroller while 4.2 V was a HIGH microcontroller. The input voltage was limited until 5V because it was the highest voltage from the microcontroller. The results showed that at 0.8 V input, the solenoid was inactive which meant it could not work in LOW voltage, whereas at 4.2 V it worked, as well as 9 V and 12 V input. In other words, solenoid worked at HIGH voltage input with such as 9 V and 12 V voltages.

TABLE 6 SMS DELIVERY TEST RESULTS

No.	Text Sent	Received Text
1.	Pengujian 1	
2.	Pengujian 2	
3.	Pengujian 3	
4.	Pengujian 4	
5.	Pengujian 5	

The SMS delivery test, as shown in the above table, the character that was sent followed the desired coding. For example, the first text sent ‘Pengujian 1’ and the received text was ‘Pengujian 1’. The duration that was needed in sending the SMS can be observed in Table 5.

TABLE 7 DURATION TEST RESULTS

No.	Activity	Duration (s)					Average (s)
		1	2	3	4	5	
1.	Delivering SMS	120	60	60	60	45	69
2.	Calling	3	3	4	3	3	3.2

This test was performed to find whether the GSM module worked to send SMS and call well or not. The test was conducted by measuring the required duration in texting and calling. The samples were used five times, and the average duration was found using the below equation:

$$Averaga\ (s) = \frac{Total\ Tests\ 1+2+3+4+5}{Total\ Tests}$$

From the above formulation, the average duration that was needed to deliver the SMS was 69 seconds. The first test required a longer duration due to initialisation. For calling test, the average duration was 3.2 seconds. From the results, it could be concluded that the GSM module required more extended time to deliver the SMS compared to call, which required 3.2 seconds on average from all five tests and connected.

TABLE 8 OPENING THE DOOR FROM THE INSIDE TEST RESULTS

No.	Activity	Required Duration (s)	Active Solenoid Duration (s)
1.	Test 1	0.40	5
2.	Test 2	0.40	5
3.	Test 3	0.39	5
4.	Test 4	0.38	5
5.	Test 5	0.40	5

This test aimed to find the performance of opening the door from the inside. To did that, this device used the Normally Open type push button. The required duration was less than 0.40 second, or it could be said that the solenoid instantly active when the button was pushed. Solenoid duration was set in 5 seconds active before it returned to its original position. This test concluded that the device worked well to open the door from the inside.

TABLE 9 OVERALL SYSTEM TEST RESULTS

No	PIN	Sensor Condition		GSM Module	LCD	Buzzer	Door
		Fingerprint Sensor	Magnetic Sensor				
1	B	TC*	TA	Calling	"Blocked system."	ON	TP
2	B	C	TA	Delivering SMS "Opened door"	"Opened door"	OFF	TB
3	S*	-	TA	Calling	"Blocked system."	ON	TP
4	B	TC*	A	Calling	"Forced entry!!!"	ON	TB**
5	S*	-	A	Calling	"Forced Entry!!!"	ON	TB**

Note:
B = Correct C = Correct A = Active
TB = Opened S = Wrong TC = Incorrect
TA = Inactive TP = Closed
* = Performed 5 times .
** = Door opened, inactive solenoid

Five conditions could occur in the overall tests. However, there should be eight conditions. Because the system unable to read the correct PIN, there could only five conditions occurred. These conditions can be observed in the above table. The first condition was the correct PIN but incorrect fingerprint scan for five times so the magnet sensor became inactive and the system called the registered phone number and the LCD displayed 'Blocked system' text. Then, the system became dormant for 60 seconds, the buzzer went off, and the door was unable to be opened. The second condition was the correct PIN and fingerprint. The magnet sensor became inactive and the system delivered a text of 'Door opened', LCD displayed 'Door opened', the buzzer did not go off, and the door was opened. The third condition was when the PIN was incorrectly entered five times, so it could not scan. The magnet sensor was inactive; the system performed a call, and the LCD displayed 'Blocked system'. The system was dormant for 10 minutes, the buzzer went off, and the door was still closed. The fourth condition was correct PIN but incorrectly scanning for five times. The magnet sensor became active, the system performed a call, LCD displayed 'Forced entry!!!', the buzzer went off, and the door was opened. However, the solenoid was inactive because it was indicated that there was a forced entry without scanning process. The fifth condition was incorrect PIN for five times, unable to scan, magnetic sensor became active, the system performed a call, the LCD displayed 'Forced entry!!!'. The next step was to conduct the same steps as the fourth condition. In conclusion, the device worked well as expected.

4. Conclusion

The assembled security system still could be developed from the hardware and the software aspects to support a better system as required. Several suggestions to be considered among others: (1) Replacing the solenoid with 5V solenoid to minimise the increase and decrease of voltage, (2) could be added with a backup battery so that the system could be used during a power outage.

References

[1] Y. Zhuo and S. Solak, "Optimal Policies for Information Sharing in Information System Security," *Eur. J. Oper. Res.*, p. S0377221719310197, Dec. 2019, doi: 10.1016/j.ejor.2019.12.016.

[2] F. De Rango, G. Potrino, M. Tropea, and P. Fazio, "Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks," *Pervasive Mob. Comput.*, vol. 61, p. 101105, Jan. 2020, doi: 10.1016/j.pmcj.2019.101105.

[3] J. E. Hachem, V. Chiprianov, M. A. Babar, T. A. Khalil, and P. Aniorte, "Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems," *J. Syst. Softw.*, vol. 162, p. 110484, Apr. 2020, doi: 10.1016/j.jss.2019.110484.

[4] M. Grimes and J. Marquardson, "Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions," *Decis. Support Syst.*, vol. 119, pp. 23–34, Apr. 2019, doi: 10.1016/j.dss.2019.02.010.

[5] H. Ai and X. Cheng, "Research on embedded access control security system and face recognition system," *Measurement*, vol. 123, pp. 309–322, Jul. 2018, doi: 10.1016/j.measurement.2018.04.005.

[6] S. Yang *et al.*, "Security situation assessment for massive MIMO systems for 5G communications," *Future Gener. Comput. Syst.*, vol. 98, pp. 25–34, Sep. 2019, doi: 10.1016/j.future.2019.03.036.

[7] R. M. Luque-Baena, D. Elizondo, E. López-Rubio, E. J. Palomo, and T. Watson, "Assessment of geometric features for individual identification and verification in biometric hand systems," *Expert Syst. Appl.*, vol. 40, no. 9, pp. 3580–3594, Jul. 2013, doi: 10.1016/j.eswa.2012.12.065.

[8] M. Adán, A. Adán, A. S. Vázquez, and R. Torres, "Biometric verification/identification based on hands natural layout," *Image Vis. Comput.*, vol. 26, no. 4, pp. 451–465, Apr. 2008, doi: 10.1016/j.imavis.2007.08.010.

[9] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, p. 113114, Apr. 2020, doi: 10.1016/j.eswa.2019.113114.

[10] M. Gomez-Barrero and J. Galbally, "Reversing the irreversible: A survey on inverse biometrics," *Comput. Secur.*, vol. 90, p. 101700, Mar. 2020, doi: 10.1016/j.cose.2019.101700.

[11] S. Bharadwaj, H. S. Bhatt, M. Vatsa, and R. Singh, "Periocular biometrics: When iris recognition fails," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Washington, DC, USA, 2010, pp. 1–6, doi: 10.1109/BTAS.2010.5634498.

[12] P. Porwik, R. Doroz, and K. Wrobel, "An ensemble learning approach to lip-based biometric verification, with a dynamic selection of classifiers," *Expert Syst. Appl.*, vol. 115, pp. 673–683, Jan. 2019, doi: 10.1016/j.eswa.2018.08.037.

[13] D. Peralta *et al.*, "A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation," *Inf. Sci.*, vol. 315, pp. 67–87, Sep. 2015, doi: 10.1016/j.ins.2015.04.013.
[14] C. Mesec, "Fingerprint identification versus verification," *Biom. Technol. Today*, vol. 15, no. 9, p. 7, Sep. 2007, doi: 10.1016/S0969-4765(07)70157-1.
[15] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Gener. Comput. Syst.*, p. S0167739X19315109, Nov. 2019, doi: 10.1016/j.future.2019.10.019.
[16] M. Esteki, Z. Shahsavari, and J. Simal-Gandara, "Food identification by high performance liquid chromatography fingerprinting and mathematical processing," *Food Res. Int.*, vol. 122, pp. 303–317, Aug. 2019, doi: 10.1016/j.foodres.2019.04.025.
[17] B. Topcu and H. Erdogan, "Fixed-length asymmetric binary hashing for fingerprint verification through GMM-SVM based representations," *Pattern Recognit.*, vol. 88, pp. 409–420, Apr. 2019, doi: 10.1016/j.patcog.2018.11.029.
[18] J. Song, C. Cho, and Y. Won, "Analysis of operating system identification via fingerprinting and machine learning," *Comput. Electr. Eng.*, vol. 78, pp. 1–10, Sep. 2019, doi: 10.1016/j.compeleceng.2019.06.012.
[19] R. P. Krish, J. Fierrez, D. Ramos, F. Alonso-Fernandez, and J. Bigun, "Improving automated latent fingerprint identification using extended minutia types," *Inf. Fusion*, vol. 50, pp. 9–19, Oct. 2019, doi: 10.1016/j.inffus.2018.10.001.
[20] K. B. Raja, R. Raghavendra, and C. Busch, "Collaborative representation of deep sparse filtered features for robust verification of smartphone periocular images," in *2016 IEEE International Conference on Image Processing (ICIP)*, Phoenix, AZ, USA, 2016, pp. 330–334, doi: 10.1109/ICIP.2016.7532373.
[21] A. Selwal, S. K. Gupta, Surender, and Anubhuti, "Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry," *Perspect. Sci.*, vol. 8, pp. 705–708, Sep. 2016, doi: 10.1016/j.pisc.2016.06.065.
[22] G. Panchal and D. Samanta, "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security," *Comput. Electr. Eng.*, vol. 69, pp. 461–478, Jul. 2018, doi: 10.1016/j.compeleceng.2018.01.028.
[23] M. Su and W. Wen, "An analysis of chaos-based security solution for fingerprint data," *Optik*, vol. 125, no. 21, pp. 6530–6534, Nov. 2014, doi: 10.1016/j.ijleo.2014.08.026.