EVOLUTION IN ELECTRICAL AND ELECTRONIC ENGINEERING
e-ISSN: 2756-8458

EEEE

Vol. 5 No. 1 (2024) 252-258
https://publisher.uthm.edu.my/periodicals/index.php/eeee

Development of a Fingerprint-Based Door Lock with Database System

Pua Xin Wei[1], Khairun Nidzam Ramli[1]*

[1] *Faculty of Electrical and Electronic Engineering.*
Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Batu Pahat, Johor, MALAYSIA

*Corresponding Author: khairun@uthm.edu.my
DOI: https://doi.org/10.30880/eeee.2024.05.01.032

Article Info

Received: 14 January 2024
Accepted: 04 March 2024
Available online: 30 April 2024

Keywords

Fingerprint sensor, Door Lock, Arduino Board

Abstract

Current door access systems are facing some significant challenges, including inadequate security measures and ineffective monitoring user's activities. The existing reliance on traditional methods, such as key locks, lacks a recorded data system, compromising both individual property security and personal safety. The purpose of this paper is to introduce an innovative security device that is widely used in premises or buildings which is fingerprint sensor. As a biometric identification method, it provides verification through fingertip recognition, mitigating common problems associated with traditional keys such as loss, theft or duplication. In addition, this paper will also include the main objective, which is to design and develop a biometric-based door access system using fingerprint technology, and to implement a database to store data on the entry times of authorised users. Several important parts are described in detail, such as the materials, methods, and implementation process, using flowcharts. In addition, this paper also includes the experiments that were mainly carried out to learn more about the characteristics of related topics, such as evaluate the performance of the system.

1. Introduction

Nowadays, fingerprints are a dependable biometric feature with a wide range of authentication applications. Many situations required us to make a verification, such as access control, classroom attendance, and financial transactions, among others [1]. Biometric technology has been successfully implemented in educational institutions, not only for identifying students and managing access and personal data but also for enhancing teaching, learning, and other processes [2].

This technology works by analyzing the unique physical or behavioral characteristics of individuals to authenticate their identity [3]. The fingerprint sensor captures personal hand geometry data, which is used as the biometric code in the management system, making it difficult for others to replicate the records [4]. However, fingerprint databases pose challenges due to their large size and the presence of noisy and distorted query images. Fingerprint images often contain distortions caused by skin elasticity [5]. Although fingerprint systems have their challenges, they are still widely used and preferred for some reasons. One key reason is ease of use, as fingerprint recognition is a non-intrusive and user-friendly biometric method, and speed of enrolment, as it is typically a fast and efficient process. In addition, fingerprint systems can be relatively inexpensive to implement and maintain compared to some other biometric technologies.

A Fingerprint-Based Door Lock with Database System could be developed in universities and aims to provide a secure and efficient way for university students to access their dorm rooms. The system uses a fingerprint sensor

Evolution in Electrical and Electronic Engineering Vol. 5 No. 1 (2024) p. 252-258

to grant access to authorised users and stores data on entry and exit times in a database. This data can be accessed remotely to monitor, manage, and identify security concerns.

2. Design and Implementation

This section comprehensively outlines the entire implementation process of the work, covering three key components. The first part, hardware implementation, details the manual creation of circuit connections from scratch. The second part, the software implementation, explains the software used to make the system a reality and ensure that it works as intended. Finally, System Operation details and clarifies the entire process of the system's functionality, providing a thorough understanding of its operational intricacies.

2.1 Hardware Implementation

In configuring the hardware setup, establish robust connections between the fingerprint sensor and the ESP32 microcontroller. Connect the VCC pin of the fingerprint sensor to the Vin pin on the ESP32 for power supply and create a common ground by linking the GND pin of the fingerprint sensor to the GND pin on the ESP32. Ensure seamless communication by connecting the TX and RX pins of the fingerprint sensor to the D17 and D16 pins on the ESP32, respectively. Integrate a relay by connecting its pin to the D32 pin on the ESP32, enabling control over external devices. For the OLED display, connect its SDA and SCL pins to the D21 and D22 pins on the ESP32, respectively, ensuring smooth data transmission. Power the OLED by connecting its VCC pin to the ESP32's 3.3V output and establish a ground connection through the OLED's GND pin to the ESP32's ground. This comprehensive setup ensures efficient communication and power distribution among the fingerprint sensor, relay, OLED display, and the ESP32 microcontroller as shown the Fig. 1.

2.2 Software Implementation

The operation of the system will start with the enrollment of the fingerprint by using the Adafruit fingerprint sensor.

First, set up a fingerprint reader circuit. Import an open-source library into the Arduino IDE and upload the code to the ESP32 board. After successful upload, establish communication with the ESP32 via the COM port. The serial monitor will guide the user to start the enrolment by assigning an ID from 1 to 127. Place a finger on the sensor, wait for the light to go out and remove the finger. Then, repeat again for confirmation to store in the sensor's ROM. If the match is successful, a confirmation message will appear, indicating completion with data stored in the sensor's ROM. If another finger is detected, the process will fail**,** and the user will be prompted to retry to enroll shown in Fig. 2. Then, another further developed main function code will be uploaded to the ESP32 to fulfill the objective of the study.

2.3 System Operation

As shown in Fig. 3, the system starts with the solenoid lock in an open circuit state, referred to as 'locked'. The ESP32 then checks the status of the sensor connection. If the sensor is not connected, the OLED display will show "Sensor Not Connected" and wait patiently for the sensor to be connected. Once the sensor is connected to the ESP32 board, the ESP32 establishes a Wi-Fi connection using pre-configured credentials stored in its ROM via the Arduino code. If a Wi-Fi connection is not established, the system will persistently scan until a connection is made. The OLED display will then show a fingerprint image with the status "Waiting for a valid fingerprint". If a fingerprint is detected, the matching process will determine if the fingerprint is stored in the ESP32's ROM. The solenoid unlocks when the IN pin of the relay receives a 5V high level voltage, completing the closed circuit. The mechanism of the solenoid, driven by an electromagnetic field, facilitates the conversion of electrical energy into mechanical motion, allowing the door to be unlocked. The OLED display briefly shows "Door unlocked, welcome" for approximately 3 seconds. During this time, the solenoid returns to an open circuit state, securing the door again, and the display shows "Door Closing". At the same time, the detected fingerprint ID and timestamp are transmitted and recorded in a Google spreadsheet. In addition, a button on the other side of the door provides an alternative method of unlocking the solenoid directly, bypassing the whole process for convenience.

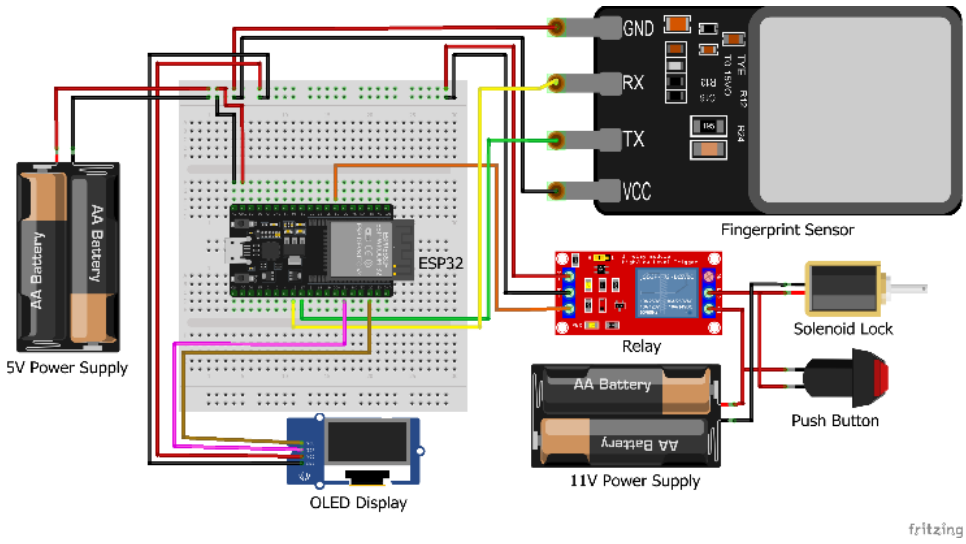

Fig. 1 *The hardware connection of the system.*

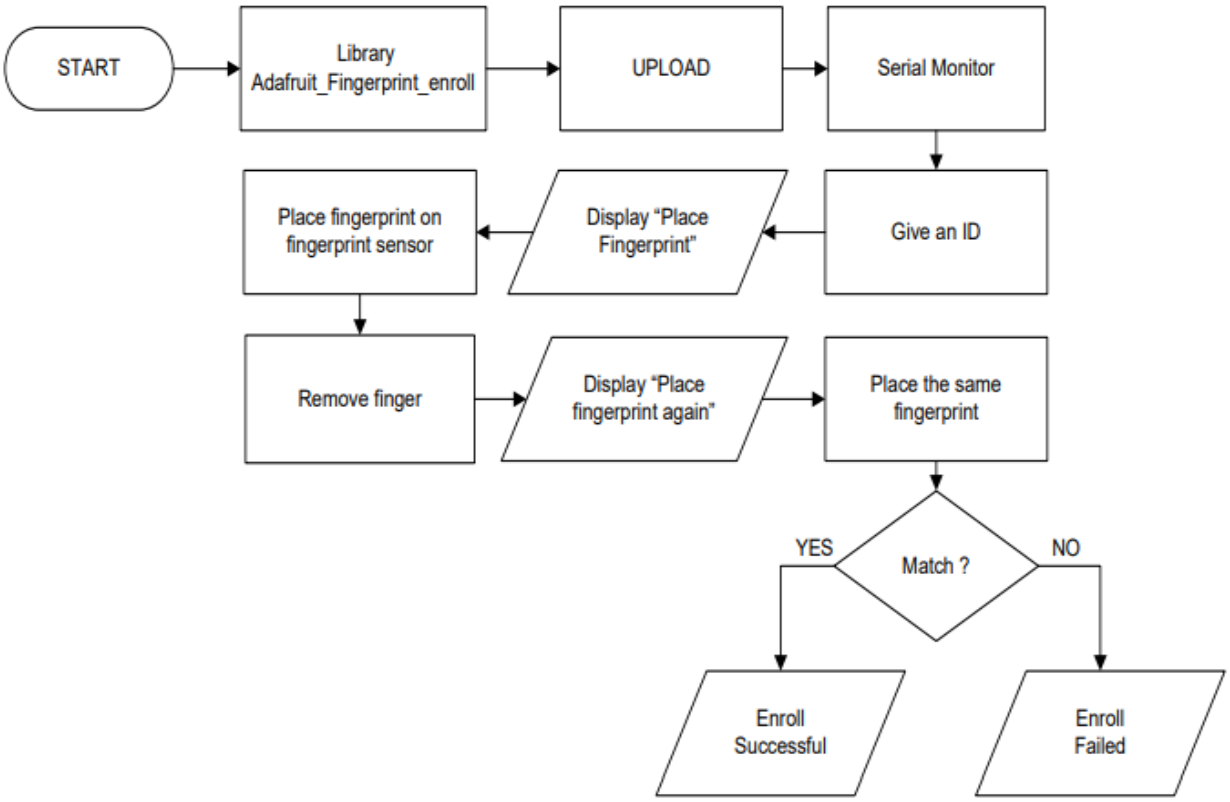

Fig. 2 *Flow chart for the enroll process of fingerprint.*

Evolution in Electrical and Electronic Engineering Vol. 5 No. 1 (2024) p. 252-258

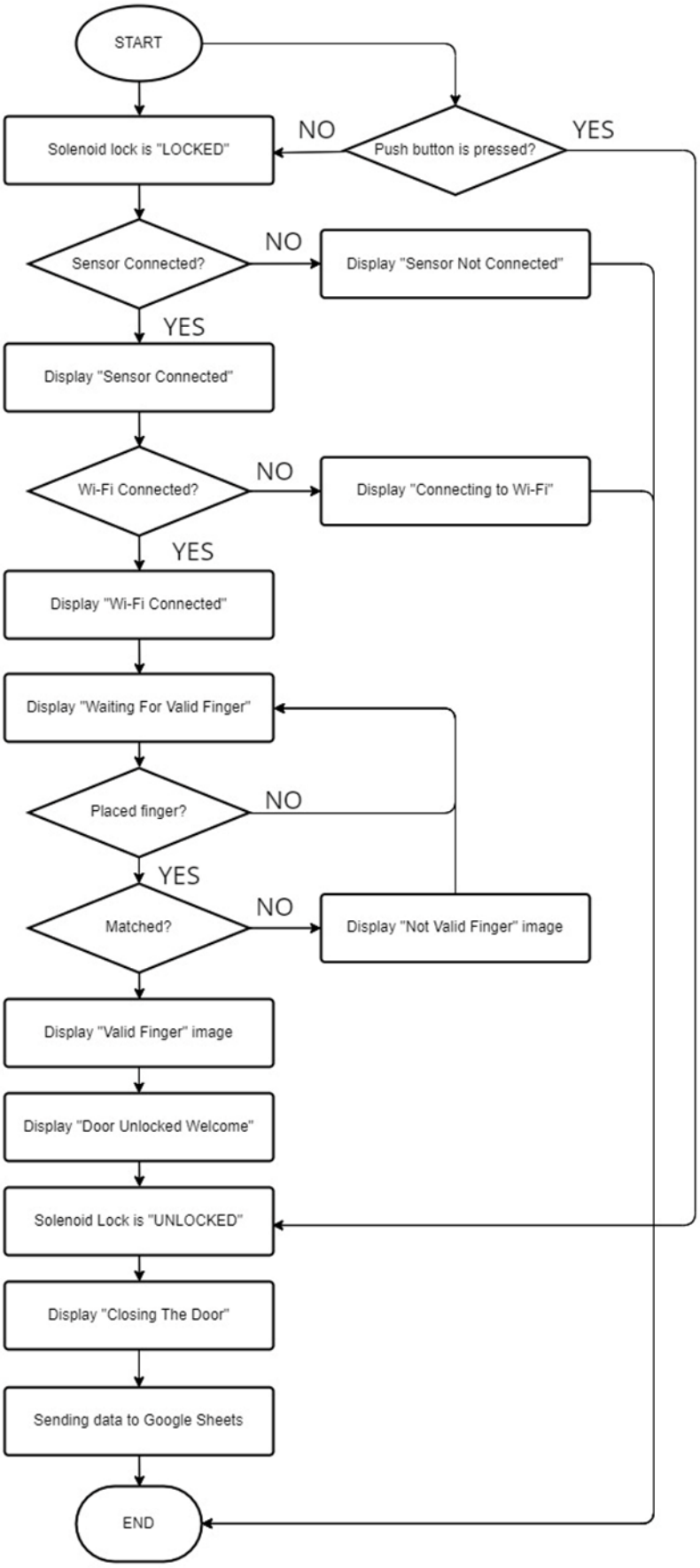

Fig.3 *Flow chart for the operation of system.*

3. Results and Discussion

In this section, discussion about the result and analysis after a few experiments were conducted to identify how the system behaved upon completion.

Table 1 *The result of the recorded fingerprint accuracy test.*

Finger ID	Finger	Number of tests	Success enrolls	Success record
#1	1	10	10	10
#2	2	10	10	10
#3	3	10	10	10
#4	4	10	10	10
#5	5	10	10	10
#6	6	10	10	10
#7	7	10	10	10
#8	8	10	10	10
#9	9	10	10	10
#10	10	10	10	10

In Table 1, it is illustrated that the experiment with the use of ten fingers, each assigned a FingerID from #1 to #10. The testing procedure was conducted 10 times for each finger, accumulating to a total of 100 test instances for the entire testing process. Across all these trials, each finger was consistently and accurately detected by the Adafruit fingerprint sensor. Moreover, following successful enrollment, the solenoid mechanism was reliably activated, leading to the unlocking of the system. Besides that, all FingerID data has been synchronized to the Google Sheet including the FingerID and Timestamp.

Table 2 *The result of the testing process using an unrecorded finger.*

Unrecorded Finger	Number of tests	Success enrolls	Success record
1	10	0	0

Table 2 shows an extra test was conducted using an unrecorded finger ID. This specific test proved unsuccessful, as the system failed to recognize the unrecorded fingerprint. Then, the door lock remained secured, highlighting the system's capability to differentiate between recorded and unrecorded fingerprints, preventing unauthorized access. Following this, upon successful enrollment, the solenoid mechanism reliably activated, resulting in the effective unlocking of the system for recognized fingerprints.

Table 3 *Total number of cases*.

	True Positives (TP)	True Negatives (TN)	False Positives (FP)	False Negatives (FN)
Total	100	10	0	0

The evaluation of results is conducted using a confusion matrix, a foundational tool in classification analysis as shown in Table 3. This matrix provides a machine learning model's prediction, distinguishing between True Positives (TP), the number of valid fingers correctly identified; True Negatives (TN), the number of invalid finger correctly identified; False Positives (FP), the number of invalid finger incorrectly identified as successful; and False Negatives (FN), the number of valid finger incorrectly identified as unsuccessful. In the provided confusion matrix, where 100 True Positives (TP) and 10 True Negatives (TN) are observed, the system demonstrates exemplary performance.

Equation (1) to (4) show the formula to calculate the accuracy, precision, recall and F1 score of the system. Based on the formula, the Accuracy, Precision, Recall, F1 Score is equal to 1. From the result of Accuracy, Precision, Recall, F1 Score, it is proven that the system operates with a remarkable level of accuracy and consistency based on 110 tests. The Accuracy, Precision, Recall, F1 Score might be lower when increasing the number of tests.

$$Accuracy = \frac{(TP + TN)}{(FP + FN + TP + TN)} \tag{1}$$

$$Precision = \frac{(TP)}{(FP + TP)} \tag{2}$$

Evolution in Electrical and Electronic Engineering Vol. 5 No. 1 (2024) p. 252-258

$$Recall = \frac{(TP)}{(TP + FN)} \tag{3}$$

$$F1\ Score = \frac{2(Precision \times Recall)}{(Precision \times Recall)} \tag{4}$$

3.1 Tested Result

As shown in Table 4, after the valid finger test experiment, the timestamp and valid finger ID were successfully stored in Google Sheet. Since the invalid finger is not stored in the ROM of the fingerprint sensor during the enrolment process, the fingerprint sensor successfully identifies the invalid finger as an invalid access. As a result, the invalid finger is not stored in Google Sheet.

Table 4 *Tested result of valid finger.*

timeStamp	FingerID
2023-11-16 15:13:55	1
2023-11-16 15:14:10	1
2023-11-16 15:14:21	1
2023-11-16 15:14:34	1
2023-11-16 15:14:55	1
2023-11-16 15:15:19	1
2023-11-16 15:15:44	1
2023-11-16 15:16:04	1
2023-11-16 15:16:20	1
2023-11-16 15:16:33	1
2023-11-16 15:16:46	2
2023-11-16 15:16:59	2
2023-11-16 15:17:11	2
2023-11-16 15:17:24	2
2023-11-16 15:17:40	2
2023-11-16 15:17:54	2
2023-11-16 15:18:09	2
2023-11-16 15:18:20	2
2023-11-16 15:18:32	2
2023-11-16 15:18:47	2
2023-11-16 15:18:59	2
2023-11-16 15:19:27	3
2023-11-16 15:19:39	3
2023-11-16 15:19:53	3
2023-11-16 15:20:08	3
2023-11-16 15:20:21	3
2023-11-16 15:20:34	3
2023-11-16 15:20:46	3
2023-11-16 15:20:59	3
2023-11-16 15:21:15	3
2023-11-16 15:21:27	3
2023-11-16 15:21:41	3
2023-11-16 15:22:00	4
2023-11-16 15:22:12	4
2023-11-16 15:22:25	4
2023-11-16 15:22:39	4
2023-11-16 15:22:52	4
2023-11-16 15:23:06	4
2023-11-16 15:23:19	4
2023-11-16 15:23:33	4
2023-11-16 15:23:44	4
2023-11-16 15:23:57	4
2023-11-16 15:24:16	4
2023-11-16 15:24:28	5
2023-11-16 15:24:39	5
2023-11-16 15:24:53	5
2023-11-16 15:25:06	5
2023-11-16 15:25:19	5
2023-11-16 15:25:36	5
2023-11-16 15:25:52	5
2023-11-16 15:26:05	5
2023-11-16 15:26:20	5
2023-11-16 15:26:31	5
2023-11-16 15:26:49	5
2023-11-16 15:27:06	6
2023-11-16 15:27:18	6
2023-11-16 15:27:35	6
2023-11-16 15:27:47	6
2023-11-16 15:27:58	6
2023-11-16 15:28:10	6
2023-11-16 15:28:27	6
2023-11-16 15:28:39	6
2023-11-16 15:28:52	6
2023-11-16 15:29:10	6
2023-11-16 15:29:23	6
2023-11-16 15:29:45	7
2023-11-16 15:29:59	7
2023-11-16 15:30:15	7
2023-11-16 15:30:26	7
2023-11-16 15:30:37	7
2023-11-16 15:30:55	7
2023-11-16 15:31:08	7
2023-11-16 15:32:06	7
2023-11-16 15:32:21	7
2023-11-16 15:32:33	7
2023-11-16 15:32:46	7
2023-11-16 15:32:57	8
2023-11-16 15:33:09	8
2023-11-16 15:33:21	8
2023-11-16 15:33:36	8
2023-11-16 15:33:49	8
2023-11-16 15:34:02	8
2023-11-16 15:34:19	8
2023-11-16 15:34:34	8
2023-11-16 15:34:56	8
2023-11-16 15:35:08	8
2023-11-16 15:35:20	8
2023-11-16 15:35:42	9
2023-11-16 15:35:53	9
2023-11-16 15:36:05	9
2023-11-16 15:36:24	9
2023-11-16 15:36:36	9
2023-11-16 15:36:47	9
2023-11-16 15:37:01	9
2023-11-16 15:37:21	9
2023-11-16 15:37:32	9
2023-11-16 15:37:46	9
2023-11-16 15:37:59	9
2023-11-16 15:38:25	10
2023-11-16 15:38:40	10
2023-11-16 15:38:52	10
2023-11-16 15:39:07	10
2023-11-16 15:39:19	10
2023-11-16 15:39:32	10
2023-11-16 15:39:45	10
2023-11-16 15:40:01	10
2023-11-16 15:40:14	10
2023-11-16 15:40:28	10
2023-11-16 15:40:40	10

4. Conclusion

In summary, the work successfully designed a biometric dormitory access system using fingerprint technology, implemented a Google Sheets database to store access times, and evaluated performance using a confusion matrix. The integrated system provides secure access control**,** and the choice of Google Sheets ensures scalability and ease

of use. This system has both strengths and weaknesses. The cost-effectiveness of the system makes it accessible and practical to implement. However, a notable limitation lies in the system's deficiency in facial recognition and tracking capabilities, given its absence of a camera component and the inability to facilitate remote access control directly. The system shows flexibility, allowing it to be adapted to different contexts and needs. Overall, the system demonstrates a practical application for improving dormitory security.

Acknowledgement

The authors would also like to thank the Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia for its assistance.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

References

[1] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani and V. K. Mittal, "Fingerprint biometric based Access Control and Classroom Attendance Management System," *2015 Annual IEEE India Conference (INDICON), New Delhi, India, 2015*, pp. 1-6. https://doi.org/10.1109/INDICON.2015.7443699

[2] Hernandez-de-Menendez, M., Morales-Menendez, R., Escobar, C.A. et al. Biometric applications in education. *Int J Interact Des Manuf 15, 365–380 (2021).* https://doi.org/10.1007/s12008-021-00760-6

[3] J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017*, pp. 1-6. https://doi.org/10.1109/CCWC.2017.7868448

[4] T. -C. Li, H. -W. Wu and T. -S. Wu, "The Study of Biometrics Technology Applied in Attendance Management System," *2012 Third International Conference on Digital Manufacturing & Automation,* Guilin, China, 2012, pp. 943-947. https://doi.org/10.1109/ICDMA.2012.223

[5] Ratha, N. K., Karu, K., Shaoyun Chen, & Jain, A. K. (1996). A real-time matching system for large fingerprint databases. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8), 799–813. https://doi.org/10.1109/34.531800