Design and Development of a Fingerprint Based Exam Hall Authentication System

Thangavel Bhuvaneswari[1], J.Emerson Raja[2], V.Chitra[3], Ng Eng Chiat[4]

[1]Faculty of Engineering and Technology, Jalan Ayer Keroh Lama, Multimedia University,75450 Melaka,Malaysia
t.bhuvaneswari@mmu.edu.my

[2]Faculty of Engineering and Technology, Jalan Ayer Keroh Lama, Multimedia University,75450 Melaka,Malaysia
emerson.raja@mmu.edu.my

[3]Department of Electrical Engineering and Renewable Energy,Oregon Institute of Technology,USA
Chitra.venugopal@oit.edu

[4]Faculty of Engineering and Technology, Jalan Ayer Keroh Lama, Multimedia University,75450 Melaka,Malaysia

Abstract: ***Fingerprint exam hall authentication system is a system designed to allow valid users to the exam hall and block invalid users after their fingerprint scan authentication. This system offers an alternative solution to conventional paper type exam authentication. Besides, this system can also be utilized as an attendance system by storing and comparing the database of the students. Traditional paper type exam authentication and attendance list is sometimes regarded as unreliable due to paper lost or proxy attendance system. This system has been running with a R305 fingerprint scanner module and an ATmega328P microcontroller main board connected with several inputs/outputs. Barrel type push buttons are the inputs and LCD, buzzer and solenoid are the outputs used in the design. The system can be operated by push buttons or using Android app to control several operations such as fingerprint enrollment, verification and deletion. The Android app operates in similar way wirelessly by connecting to Bluetooth module but it has additional feature such as student attendance databases management and storing as well as PDF file export. The design can be operated as standalone and handheld method with both hardware and Android app is successfully implemented by using the prototype.***

Keywords**: Finger print, Authentication system, Exam, biometric technique, Android App.**

(Article history: Received: March 2022 and accepted May 2022)

I. INTRODUCTION

Traditional attendance booklet is unreliable as it is easy to get stolen, lost or damaged. In addition, some students may tend to help their friends to take their attendance by imitating their signatures. Besides, it is very time consuming for an exam invigilator or a lecturer keeps tracking of students' attendance by counting the attendance slips or make a roll call in a class. Therefore, it is important to look for alternative system to handle the attendance system. Biometeric authentication system like face recognition, voice recognition and eye (iris) recognition are commonly used. Fingerprint recognition is the most popular and commonly used biometric techniques among other techniques. The potential benefit of the fingerprint-based exam hall authentication system in an educational institution and organization cannot be overlooked. This system is used to replace traditional exam hall authentication and attendance booklet with the benefits of saving time and eliminating all of drawbacks of the attendance booklet.

The fingerprint is made up unique patterns which consist of lines called ridges and space called valleys. This unique pattern provides good reliability compared to other conventional techniques. Hence fingerprint is used for authentication system. Fingerprint authentication is a method to verify a fingerprint matching among multiple fingerprints in a database.

The fingerprint authentication system needs to be placed in exam hall or classroom, then students are required to place their fingerprint on the scanner to show their presence in the exam or classroom. Prior to this students' fingerprint are collected and stored in the database and then classified them into each exam venue and classroom that they belong to. This can be realized by using the Android app feature which is able to manage the students' profile associated with each fingerprint database.

Fingerprint is the impression of the ridges and furrows made by human fingers which provides unique and permanence features. The ridge and furrow patterns were formed on the finger and skin of the palm since we were born. Fingerprints are differentiated by the feature named Minutiae which exhibits anomalies on the ridges however not by the ridges and furrows. There are two important minutiae type among them. One is ridge ending that is the abrupt end of the ridge. Other one is ridge bifurcation defines as two ridges are divided from a single ridge.

Fingerprints have very high levels of reliability and have been widely used for criminal investigation by forensics expert[1]. Besides that, fingerprints have been used as a common means of identification for a very long time.

Fingerprint recognition is the process of comparing known or unknown fingerprint among the other fingerprints in the database to carry out the matching process. The recognition process can be categorized into identification and verification.

One's identity is specified based on his fingerprint by using fingerprint identification technique. The information regarding the identity of a person is not stored after the fingerprint is captured. Then, the fingerprint is matched among numerous fingerprints stored inside the database. If there is a match found with the fingerprint existed in the database, then the identity of that particular person is retrieved. This indicates the method of one-to-n matching through comparison of one capture of fingerprint with other captures in the database. The fingerprint identification technique is using widely for criminal cases.

Another method is fingerprint verification where a person's identity stored in a database after his fingerprint is captured. The identity of the person is retrieved back when the real time captured is occurred on enrolling the fingerprint. This illustrates a one-to-one matching process. This method has been widely adopted in offices like passport department as a person's identity needs to be verified and checked with the fingerprint provided in an earlier stage.

The fingerprint based attendance management system is introduced by L. S. Ezema et al.from Electrical Power and Electronic Development Department, Projects Development Institute (PRODA), Enugu, Nigeria in ref[3]. This fingerprint attendance system was designed to carry out operation as a hand-held and standalone system by not using the computer that differs from other fingerprint attendance systems.

A software was designed by using Visual Basic programming that is capable to record initial attendance by exporting the database in Microsoft Excel. In addition, it can be used to register each new user and accept the attendance record from the hardware(AT89S52 microcontroller, fingerprint scanner, 20x4 LCD Display, real time clock). If necessary, the updated attendance record can be printed by compilation with the hardware.

The hardware design of Embedded fingerprint identification system is proposed by Jinhai Zhang from Marine college of Shandong jiaotong university, Weihai, Shandong, China [4]. The system consists of control master module, fingerprint collection module, USB interface and fingerprint recognition algorithm. The architecture of the fingerprint recognition system includes core processor, DSP algorithm module and P89C52 microcontroller CMOD (control module) in relation to the main controller.

For the hardware implementation in this system, microcontroller ATMEL P89C52 with regards to the control module is used to interface PC communication and the DSP communication on account of user interaction. To enroll and login actions, the LCD Display and keyboard were connected to the controller and communicated with the DSP as well. DSP processor mainly deals with fingerprint collection, preprocessing, and the fingerprint matching algorithm software [4].

Two researchers from Department of E&TC, Pimpri Chinchwad College of Engineering, Pune, India in ref[5] had developed the automatic fingerprint authentication system and implemented a fingerprint recognition algorithm with Spartan-6 FPGA. This system involved hardware and software collaborative design serve as two fingerprint minutiae capture matching system.

The working principle of the system was involved in two stages. First stage is related to enrollment stage and second stage is about authentication stage. User's fingerprint features are taken and stored in the database as a fingerprint template in enrollment stage. The fingerprint features are verified and compared with the templated stored in the database during identification or authentication stage. Eventually, the authentication result was output by the system.

First hardware implementation which is Microblaze processor on Spartan 6 FPGA has the characteristic of reduced instruction set computer (RISC) based on Harvard architecture [6]. C programming was used in developing the program through the use of Software Development Tool (SDK) and run on Microblaze processor as a matching algorithm for the system. The processor then takes the two extracted fingerprint capture templates and compares with other templates through the execution of matching algorithm. Matching scores were sent to laptop by FPGA and the results were displayed in HyperTerminal on system.

Advanced Fingerprint Authentication System in Two Wheelers system was developed and created by researchers in ref[7]. It is a fingerprint authentication system designed for two-wheelers which its main purpose is thefts prevention for two-wheelers. The fingerprint system had replaced the conventional self-start method of the two-wheeler. The hardware used for the system are AVR microcontroller ATMEGA328, fingerprint scanner module R305, Fuel sensor and GSM Module.

The vehicle ignition system is started by the hardware module. The essential concept of this system is valid fingerprint will ignite the vehicle whereas invalid fingerprint causes the vehicle unable to start. The system will check for the validity of the fingerprint once the fingerprint is acquired by the fingerprint scanner module. If the fingerprint template has been stored in the database, then it will pass the matching process after comparison. Then sufficient fuel will be provided to the two-wheelers after the ignition system is launched. In case of invalid fingerprint found, the vehicle owner will be notified and received a message via GSM module. The desired output is displayed on the LCD in the same time DC Motor is started after passing of valid fingerprint as well as when the fuel is sufficient.

Fingerprint Based Biometric ATM Authentication System was realized by researcher, Dhiraj Sunehra et. al [8]. An ATM cashbox access system prototype was implemented using a PIC16F877A microcontroller from Microchip Technology and R305 fingerprint scanner module. Embedded C programming language was used to write the software of the system and then it was tested.

First of all, the finger of bank manager is scanned and the fingerprint is stored as template afterwards for further verification while certain authentication time will be given. The matched fingerprint after authentication will trigger the ATM cashbox to be opened, however, unmatched fingerprint will cause the buzzer sound as an alarm. A user is required to register fingerprint in the database of the fingerprint scanner module to serve as an input to the controller. The fingerprint is then carried out checking and comparison process with other fingerprint template stored in previous stage. Any related and important information will be displayed on the LCD. The door is opened by the operation of DC motor when an authorized person is authenticated by the system

In Ref [9] subbulakshmi et al.proposed a finger print based exam hall authentication system. The system is meant to permit only users verified by their fingerprint scan and doesn't allow non verified users. It consists of a fingerprint scanner connected to microcontroller circuit. In registration mode the system allows to register user's information and save their identity with respective ID numbers within the system memory. After registration the person must scan his/her finger with the help of the scanner. The microcontroller checks the person's fingerprint. If the fingerprint valids the motor driver send a message to open a door.

Shilpa C et.al proposed IoT based voting system to reduce the malpractices during election[10]. The voter details along with the fingerprint is stored in database. Based on the aadhar number matching and fingerprint matching voting system have been cast.The voter can enter their native /living place using IoT platform and cast their vote for a particular candidate.

This paper is organized as follows. In section 2 methodology is explained with flow chart. In section 3 the results are discussed and in section 4 concludes the paper.

II. METHODOLOGY

The proposed block diagram of the fingerprint authentication system shown in Figure-1 has R305 fingerprint scanner module and an ATmega328P microcontroller main board connected with several inputs/outputs. Barrel type push buttons are the inputs and LCD, buzzer and solenoid are the outputs used in the design. The system can be operated by push buttons or using Android app to control several operations such as fingerprint enrollment, verification and deletion. The Android app operates in similar way wirelessly by connecting to Bluetooth module but it has additional feature such as student attendance databases management and storing as well as PDF file export.

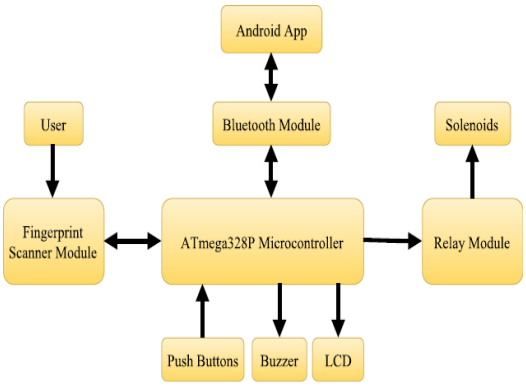

Fig. 1. Block Diagram

A. Flowchart

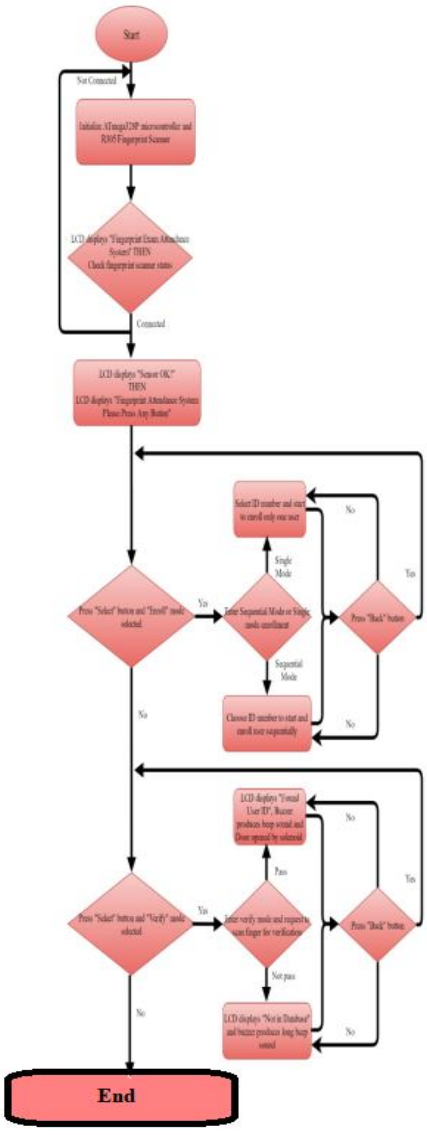

Fig. 2. Flow chart

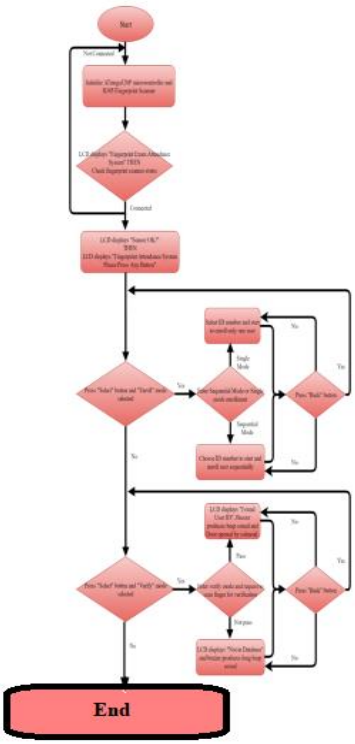

Fig. 3. Flowchart

From the flowchart as shown in Figure-2 and Figure-3 above, the ATmega328P connected with the main board and 20 x4 LCD are initialized when the power is supplied from external source. Then, the LCD will display “Fingerprint Exam Attendance System”, in the meantime, the microcontroller will check for the R305 fingerprint scanner connection status. If the fingerprint scanner is connected, then LCD will display “Sensor OK!” message and proceed to display “Fingerprint Attendance System Please Press Any Button”. If it is not connected, then LCD will display “Sensor not found.” and wait until the fingerprint scanner to connect in order to continue to next step.

While the “Select” button is pressed, “Please Select Mode” menu will be displayed, there are three modes can be selected which are “Enroll”. “Verify” and “Delete”. If “Enroll” mode is selected and entered, then two modes of the enroll mode can be selected, one is “Sequential Mode”, another one is “Single Mode”. For sequential mode, a start ID must be chosen to enroll the user sequentially, for example, if ID 8 is selected as start ID, then the user will be enrolled from ID 8, then ID 9, ID 10 until an ID to stop. In the case of single mode enrollment, an ID will be selected to enroll a user only.

After “Verify” mode is selected, the user needs to press again the “Select Button” to enter “Please Scan Finger” mode, next, the user is required to scan finger for authentication. If the user has passed the authentication process, LCD will display “Found User ID: 0” for the user which is registered under ID 0 and so on. Meanwhile, the relay module will be triggered and solenoid acts as door opening action. The LCD will display “Not in Database” if the user does not pass the authentication.

As for “Delete” mode, two modes can be selected after entering the mode which are “Delete ALL” and “Delete Single”. All the fingerprint database will be deleted if “Delete ALL” mode is entered while only one fingerprint template for selected ID will be deleted if “Delete Single” mode is entered.

“Back” button can be pressed to return to the main display menu and waiting for next operation by a user.

B. Android App Flow Chart and Interface

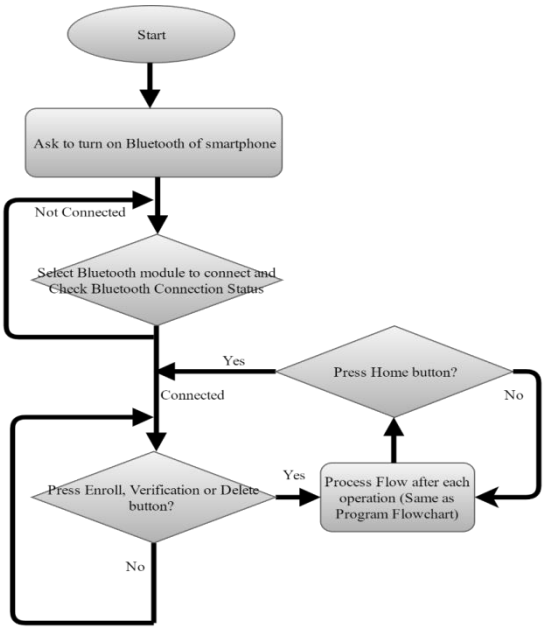

Fig. 4. App Flow chart for Enroll, Verification and Delete

Figure-4 shows the App flow chart for Enroll, Verification and Delete process. Firstly, user is asked to turn on the Bluetooth if the Bluetooth is not turned on. Figure-5 shows the request for allowing or denying to turn on the Bluetooth. Then, the HC-05 Bluetooth module must be selected for connection. Figure-6 shows the Bluetooth devices list to be selected to connect, HC-05 must be selected for this system. Otherwise, the next step cannot be proceeded. After the Bluetooth is connected, user can choose which operation to be carried out such as Enroll, Verification and Delete. Figure-7 shows the HC-05 Bluetooth is successfully connected. The next step after selecting the specific operation is the same as the Program Flow as shown in Figure-8 and Figure-9. If no operation is selected, it will remain at the user interface.

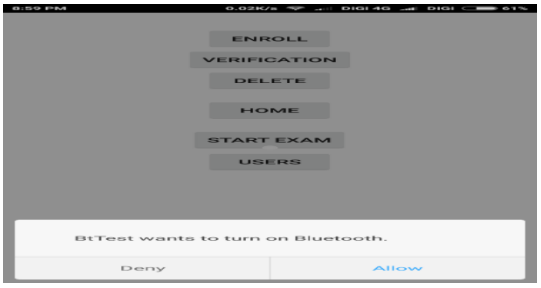

Fig. 5. App asks for turning on the Bluetooth

Fig. 6. Select Bluetooth device to connect

Fig. 7. HC-05 Bluetooth module connected successfully

Figure-8 shows request for enroll single or sequential after Enroll button is pressed. Then user can choose which ID to start enroll sequentially or enroll only single user with selected ID as shown in Figure-9.

Fig. 8. Request for enroll single or sequential

Fig. 9. Select and confirm ID to start enrolling user

For the verification operation, user is requested to scan the finger. If the fingerprint is not in database, all the details of specific user are empty as shown in Figure-10. Figure-11 shows the important detail such as user ID is not shown since it is not enrolled and same goes to other details such as Name, Matric No. and Class ID. Figure-11 shows the Finger ID is shown if the user's fingerprint is enrolled and stored in the system, but other details are blank since registration process is not finished for the user.

Fig. 10. Details are not shown for unregistered user

Fig. 11. Finger ID is shown for stored fingerprint of the user

After user has pressed Delete button, then request for Delete ALL or Delete Single will be prompted out as shown in Figure-12. If Delete Single is selected, then user needs to select an ID to delete while Delete ALL confirmation will be asked if Delete ALL is chosen as shown in Figure-13 and Figure-14.

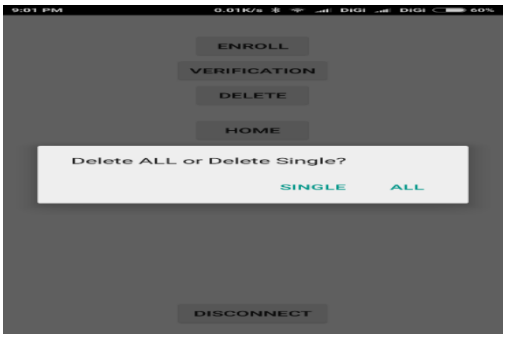

Fig. 2, Request for Delete ALL or Delete Single

Fig. 1I. Select an ID to delete

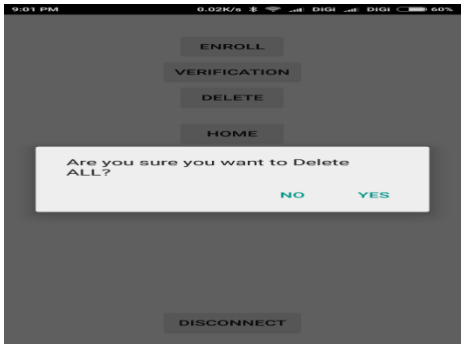

Fig. 14. Delete ALL confirmation

C. App flow chart for Users button is pressed

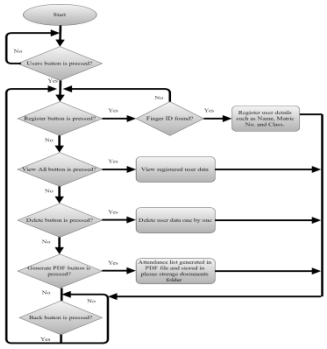

Fig. 15. App flow chart for Users button is pressed

Figure-15 shows the App flow chart for Users button is pressed. To register a user's details inside the database, the Users button must be pressed and entered, then user is required to scan the finger first to let the finger ID to be detected. To ensure the user is registered successfully, the user must enroll fingerprint earlier, then just proceed to user registration. Otherwise, situation as shown in Figure-16 will be happened. Every details are blank especially for the finger ID which is relatively important cannot be found as well. For user's fingerprint that is enrolled earlier, the Finger ID will be shown and other details can be filled and selected for registration. as shown in Figure-17. Figure-18 shows the user is successfully registered.

Fig. 16. All details are not shown if the user's fingerprint is not enrolled

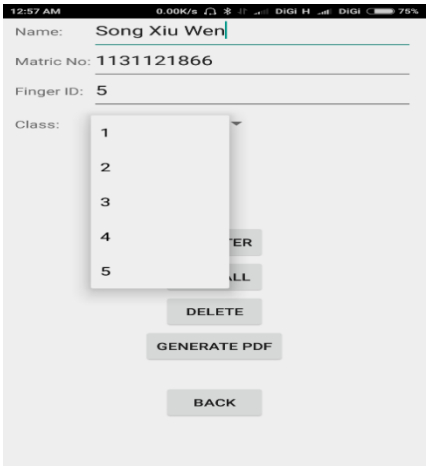

Fig. 17. Fill in user's details and select class if the user's Finger ID is found

Fig. 18. User is successfully registered

After the user registration, the user's data can be checked by pressing View All button as shown in Figure-19. All the details stored can be viewed from time to time. The "Time In: " detail there is blank as the exam is not started yet so there is no time record for the user if entering exam hall or classroom using the system.

Fig. 19. User data is checked after pressing View All button

Figure-20 shows the user data can be selected to delete one by one if Delete button is chosen. Figure-21 shows an exam attendance report can be generated in PDF format and stored inside phone storage documents folder and ask for the type of PDF viewer to open the attendance list file automatically when Generate PDF button is pressed. If the Back button is not executed, then the screen will remain at the screen being executed until operation is called back to previous screen.

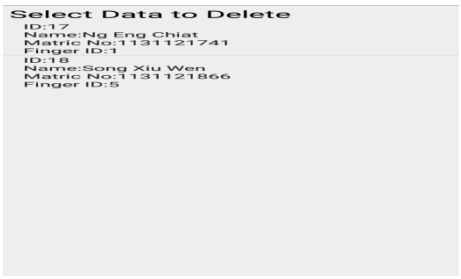

Fig. 20. Select user data to delete

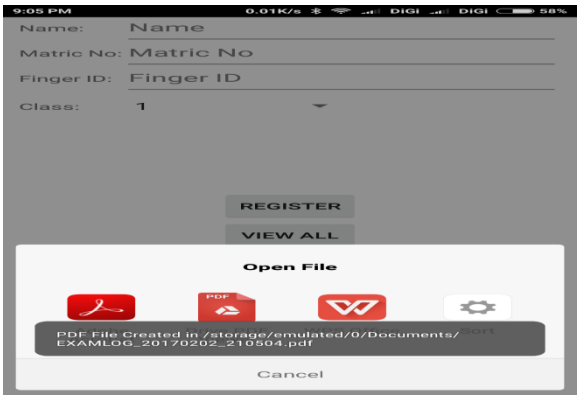

Fig. 21. Exam attendance report generated in PDF format

III. RESULTS AND DISCUSSION

All hardware components are placed and stored inside a black colour box for a better appearance in order to demonstrate the fingerprint based exam hall authentication system. Figure-22 shows the internal structure of the demonstration box that contains main board with ATmega328P microcontroller, relay module, HC-05 Bluetooth module, buzzer and input power jack. Figure-23 shows the R305 fingerprint scanner module, I2C 20x4 LCD and four-barrel type push buttons were mounted on the cover of the demonstration box. Solenoids as outputs of the system are placed outside of the box.

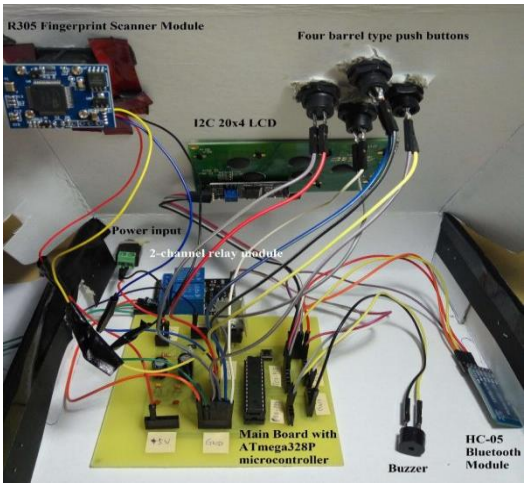

Fig. 22. Internal structure of the demonstration box

Fig. 23. Exterior of the demonstration box

Figure-24 and Figure-25 shows the user is found and passed, then sliding door is opened for 5 seconds if the user had enrolled in the system previously. The delay for the door opening duration can be changed to meet the requirement of certain criteria. Figure-26 and Figure-27 shows invalid user is not passed and the sliding door is not opened if the user's is not enrolled in the system.

Fig. 24. User ID is found and passed by the system

Fig. 25. Door is opened by solenoid pulling in action for enrolled user

Fig. 26. User is not found in the database and not passed by the system

Fig. 27. Door is not opened for not enrolled user

3.1 Android App of Fingerprint based Exam Hall Authentication System

When the exam is started after Start Exam button is executed, the users is required to scan their fingerprint for authentication. Figure-28 and Figure-29 shows the time stamp will be updated after the users scan the finger and the time in will be recorded down inside the SQLite database. Then the exam attendance report can be generated in PDF format and stored inside phone storage documents folder. The PDF can be viewed by any kind of PDF viewer installed in the smartphone. Figure-30 shows the details such as Name, Matric No., Class Name and Time In are recorded in the exam attendance report. The date and time along the Exam Attendance Report will be updated every time a new PDF file is generated.

Fig. 28. Time stamp updated for user Ng Eng Chiat

Fig. 29. Time stamp updated for user Song Xiu Wen

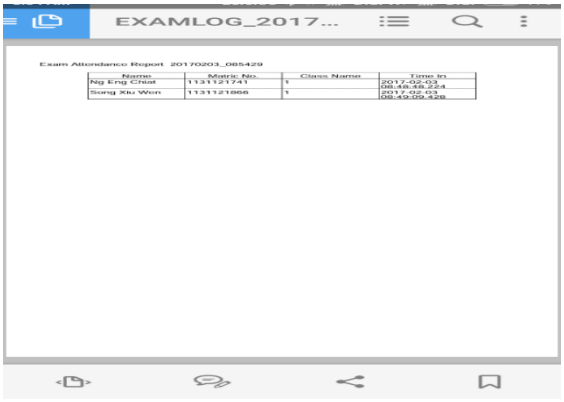

Fig. 30. Exam Attendance Report in PDF format

Figure-30 shows the user's details is not found if the user is not registered in the system although the fingerprint has been enrolled previously and the user's details will not be shown in the exam attendance report as well.

Fig. 31. User's details are not found if the user is not registered

Figure-32 shows the case if a user is registered without any details filled in, it will be stored inside the database but all the details will be empty except for user's Finger ID and class ID since these details are compulsory. Same goes to the exam attendance report which is generated afterwards.

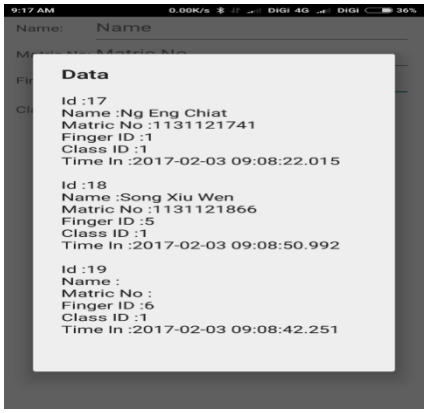

Fig. 32. User's data with Finger ID 6 can be viewed although details are missing

IV. Conclusion

Fingerprint exam hall authentication system is a system that consists of standalone hardware system and Android app which are able to control the authentication process. Beyond

that, the system can be controlled remotely by using the Android app via Bluetooth communication. HC-05 Bluetooth module acts as a communication medium between Android smartphone and ATmega328P main board so transmitting and receiving operation can be done seamless without any other configurations.

The other feature of Android app is that it is able to manage student attendance database record after they have been registered in the database. The time stamp will be updated once the registered students have scanned their fingers via the R305 fingerprint scanner. The app can supervise the attendance of the students and prevent attendance cheating case. Thus the students will be encouraged to attend their class and the whole attendance rates can be pushed up if the system is implemented. The attendance report can be generated in PDF format for reference and it will be lost easily since it is stored inside phone storage digitally.

REFERENCES

[1] D. Acharya and A. K. Mishra, "Wireless Fingerprint Based Student Attendance Sytem," no. 10602061, 2010.

[2] L. S. Ezema, J. N. Eneh, and I. Amanze, "Fingerprint Based Attendance Management System," Int. J. Sci. Eng. Res., vol. 6, no. 7, pp. 1623–1628, 2015.

[3] Z. Jinhai, "Hardware design of embedded fingerprint identification system," 2011 Int. Conf. Consum. Electron. Commun. Networks, pp. 4995–4998, 2011.

[4] A. Jain and S. Pankanti, "Fingerprint Recognition," Essent. Guid. to Image Process., pp. 649–676, 2009.

[5] A. S. Shinde and V. Bendre, "An embedded fingerprint authentication system," Proc. - 1st Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2015, pp. 205–208, 2015.

[6] X. Inc, "MicroBlaze Processor Reference Guide." [Online]. Available:http://www.xilinx.com/support/documentation/sw_manuals/xilinx14_2/mb_ref_guide.pdf.

[7] V. Khadasane, M. Desai, D. Khatavkar, and S. Lad, "' Advanced Fingerprint Authentication System in Two Wheelers ,'" Int. J. Tech. Res. Appl. e-ISSN, vol. 40, no. 40, pp. 42–45, 2016.

[8] D. Sunehra, "Fingerprint Bashttp://www.atmel.com/devices/ATMEGA328P.aspx.

[12] "How To Use Fingerprint Identification Modules." [Online]. Available: http://www.electroschematics.com/11944/how-to-use-fingerprint-identificationed Biometric ATM Authentication System," Int. J. Eng. Invent., vol. 3, no. 11, pp. 22–28, 2014.

[9] Subalakshmi.K, Thilagavathy.M, Surendhar.S, Surya.J, Balaji.S, Exam Hall Authentication Using Finger Print, International Journal of Electrical Engineering and Technology (IJEET), vol.12, no.3, 2021, pp. 88-93.

[10] Shilpa C Venugopal, Resmi K.Rajan, "IoT Based Voting Machine With Fingerprint Verification", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 1, 2020 (Special Issue)

[11] "ATmega328P." [Online]. Available: -modules/.

[13] "Finger Print Sensor (R305) [3935] : Sunrom Electronics." [Online]. Available: http://www.sunrom.com/p/finger-print-sensor-r305.

[14] "arduino-info - BlueTooth-HC05-HC06-Modules-How-To." [Online]. Available: https://arduino-info.wikispaces.com/BlueTooth-HC05-HC06-Modules-How-To.

[15] "HC-05 Master / Slave Bluetooth Module." [Online]. Available: http://www.sgbotic.com/index.php?dispatch=products.view&product_id=1939.

[16] "I2C 20x4 LCD Module - Blue Backlight | Display & Graphics | Robot R Us." [Online]. Available: https://www.robot-r-us.com/vmchk/display-graphics/i2c-20x4-lcd-module-blue-backlight.html.

[17] "SainSmart IIC/I2C/TWI Serial 2004 20x4 LCD Module Shield For Arduino UNO MEGA R3 3D Printing, Arduino, Robotics | Sainsmart." [Online]. Available: http://www.sainsmart.com/sainsmart-iic-i2c-twi-serial-2004-20x4-lcd-module-shield-for-arduino-uno-mega-r3.html.

[18] "Solenoid - 5v." [Online]. Available: http://www.myduino.com/index.php?route=product/product&product_id=452.

[19] "2 Relay Module, 5V, 10A, Opto Isolated, for Arduino/PIC/AVR." [Online]. Available: http://modtronix.com/mod-rly2-5v.html.

[20] "Arduino - Introduction," *arduino.cc*. [Online]. Available: http://arduino.cc/en/guide/introduction.

[21] X. Ducrohet, K. Chou, and T. Norbye, "Android Studio: An IDE built for Android," *Android Dev. Blog*, 2013.

[22] "Meet Android Studio | Android Studio." [Online]. Available: https://developer.android.com/studio/intro/index.html.

AUTHOR PROFILE

Dr.Thangavel Bhuvaneswari

Dr.Thangavel Bhuvaneswari is working as a Senior Lecturer in Robotics and Automation programme, Faculty of Engineering and Technology, Multimedia University (MMU), Melaka. She has 20 years of teaching experience, teaching in various disciplines of robotics and automation, telecommunication and mechanical engineering. Her research interests are digital system design, VLSI, FPGA, VHDL Modelling, Solar power controller design and bioinformatics. She has published 42 papers in reputed journals and international conferences. She has been invited for her subject matter expertise to evaluate PhD thesis and review papers in IEEE conferences. She is senior member of IEEE and member of IET.

Dr.J.Emerson Raja

Dr.J. Emerson Raja is currently working as a senior lecturing in the Faculty of Engineering and Technology at Multimedia University, Malaysia. His research work is centred on applying soft computing techniques to monitor the health of machines. He had given key note speeches in few International Conferences at China and India. He has published 25 international journal papers and 20 conference papers.