Design and Implementation of an Arduino Based Smart Fingerprint Authentication System for Key Security Locker

1st Bong Siaw Wee
Department of Electrical Engineering
Politeknik Mukah
Mukah, Sarawak, Malaysia
shaweibong2016@gmail.com

***Abstract*—Human beings have always prioritized security. Simple mechanical locks with the key as the authentication factor were among the earliest forms of security. A key is a tiny, shaped piece of metal with incisions made to match the wards of a certain lock that is placed into the lock and twisted to open or close it. People tend to misplace the keys and it is troublesome for other users to use the keys because it is hard to find the right key. Moreover, the keys are without any protection. Anyone besides the user can easily access the keys. Therefore, an Arduino Based Smart Fingerprint Authentication System for Key Security Locker was proposed and developed in this research. The Key Security Locker System is designed to make sure that the keys are stored in a more organized and effective location. Biometrics is the science of determining an individual's identification based on physical, chemical, or behavioral characteristics. The importance of biometrics in modern society has been strengthened by the necessity for large-scale identity management systems, the operation of which is dependent on the precise assessment of an individual's identity in the context of many applications. This technology recognizes authorized personal's unique fingerprints and allows them access. To utilize the fingerprint scanner, the user must place their finger on it. The event will capture new human minutiae through fingerprint scanning. These new minutiae will be compared to those in the database to determine if the individual is authorized or non-authorized. The Liquid-Crystal Display (LCD) will show "Fingerprint Match" if the fingerprint matches the fingerprint in the database. Then, the microcontroller will instruct relay and solenoid lock to unlock the locker door. If the fingerprint is not matched, the LCD will appear "Not Matching". Then, the locker door will remain locked. Hence, the proposed system provides better security, higher efficiency, and in many instances, increased user convenience due to it being built based on a biometric system.**

Keywords—Arduino UNO, Security, Key Box Locker, Biometrics, Fingerprint Authentication System

I. INTRODUCTION

Security has always been a concern of paramount importance to human beings [1]. When it comes to security, it is one of the most pressing problems in today's hectic, competitive environment, where a human being is unable to offer protection for his possessions daily. Keeping our staff safe has always been at the top of our priority list. Today's security includes a wide range of software and hardware, such as web-based security services, biometrics, and personal gadgets with built-in security levels [2].

A traditional lock with a key was the favored locking mechanism. This is an old-fashioned locking mechanism with a few flaws, such as the key being easily copied and the lock is easily opened by an unauthorized person [3]. Several approaches have been reported in the literature for security solutions such as a radio-frequency identification (RFID) card, keypad, pin, password, or Internet of Things (IoT) by unlocking the device with a mobile phone [4-8]. These systems have the same advantages and disadvantages, and this form of security lock may open the system from any security level. To unlock the system, the user either enters a Personal Identification Number (PIN) or swipes an RFID card [9]. This system lacks a security level chain, which would improve security. An RFID card, which stands for radio frequency identification, can be used to unlock the system. The scanner scans the radio frequency to determine if the identity is allowed or unauthorized. However, the primary drawback of this approach is that the passwords could be hacked and a card may be stolen or lost. As a result, the user must handle it with caution [10]. Besides, this system also has no alert system in case of a break-in, or an unauthorized person tries to unlock the door.

IoT is an abbreviation for the internet of things, which is used indoor locks through a wireless connection. The user can utilize IoT-enabled applications on his smartphone to unlock the door lock. With a single touch, the user may simply open or lock the system However, IoT is supported only by an internet connection [11, 12]. The most striking problem for those models operating with smartphones is the risk of being unable to open the door if the smartphone's battery runs out. Unfortunately, the autonomy of these gadgets is limited, and whenever the user is unable to charge their smartphone, so the user will face the risk of being unable to open the door.

Biometrics provides a natural and dependable approach to some elements of identity management by employing fully automated or semi-automated systems to recognize persons based on biological features [13, 14]. It is possible to create an identity based on who you are rather than what you own, such as an identification (ID) card, or what you know, such as passwords, by utilizing biometrics. Biometrics may be used to augment ID cards and passwords in some applications, adding

an extra layer of protection. This type of setup is sometimes referred to as a dual-factor authentication method.

Therefore, an Arduino Based Smart Fingerprint Authentication System for Key Security Locker was proposed and developed in this research. The proposed method is more efficient due to biometric identifiers cannot be readily misplaced, faked, or shared, they are regarded more trustworthy for person recognition than the traditional token (e.g. keys or ID cards) or knowledge (e.g. password or PIN) based techniques. Fingerprint technology is the most generally recognized and established biometric approach. It is the most user-friendly and puts a better level of protection at your fingertips. Fingerprint recognition improves security, increases efficiency, and increases consumer convenience. Furthermore, fingerprint recognition is the most commonly used biometric feature. It is often assumed that each finger has a distinct pattern. Given that there are around 6.5 billion live individuals in the world, and assuming that each person has ten fingers, there are 65 billion distinct fingers! Fingerprints were originally used as a form of identification over a century ago.

Fingerprint recognition is one of the most secure systems due to everyone has various forms of fingerprints, fingerprint identification. Therefore, unauthorized access can be restricted by creating a lock that saves the fingerprints of one or more authorized users and opens the system when a match is detected. The Arduino serves as a data storage device for users. the skin on our hands and soles has a flow-like pattern of ridges on each fingertip that is unique and unchangeable, biometric authorization shows to be one of the greatest features. As a result, fingerprints are a one-of-a-kind form of identification for everyone. The usage of fingerprint scanners in contemporary hand-held devices such as mobile phones and computers demonstrates their popularity and dependability.

II. METHOD

A. Block Diagram

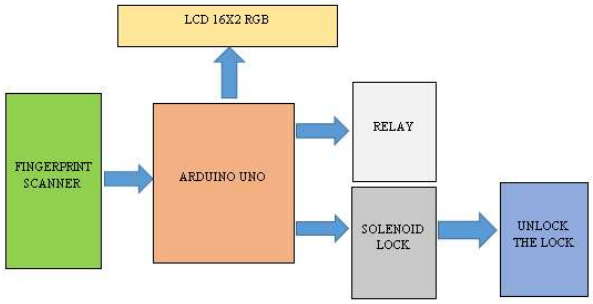


Fig. 1. Block diagram

The block diagram of an Arduino-based Smart Fingerprint Authentication System for Key Security Locker is shown in Fig. 1. To utilize the fingerprint scanner, the user must place their finger on it. The fingerprint scanner subsequently captures the fingerprint picture and sends it to the Arduino Uno. The Arduino Uno will search for the original fingerprint data that is already on the board. If the fingerprint matches one previously saved in Arduino, the Liquid-Crystal Display (LCD) will display "Fingerprint Match." The microcontroller will then instruct the relay and solenoid lock to open the locker door. If the fingerprint is not matched, the LCD will appear “Not Matching”. Then, the locker door will remain locked.

The Arduino is an open-source physical computing platform based on a single microcontroller board. The Arduino is used when there are interactions between inputs and outputs. It has 14 digital Input/Output (I/O) pins, six of which can be used as pulse width modulation (PWM) outputs, six analog inputs, a reset button, a power connector, a USB connection, and other features. It includes everything needed to support the microcontroller; simply connect it to a personal computer (PC) through a USB cable and power it up using an Alternating Current (AC)-to-Direct Current (DC) adapter or battery. It is used to control the output based on the input directives, for as utilizing a switch to control a light or motor.

The optical finger reader sensor, commonly known as a fingerprint reader. It is a piece of technological equipment that captures a digital image of the fingerprint pattern. The captured image is known as a live scan, which is then digitally processed. The distinctive characteristics of the fingerprint are extracted, and a fingerprint biometric template is generated. This biometric template has been saved and will be used for matching in the future [15].

The relay is a switch that operates electrically and consists of two main parts, namely electromagnetic (coil) and mechanical (set of switches). The electromagnet requires a low voltage to activate, which will provide via the Arduino. When once triggered, it will pull the contact to complete the high voltage circuit.

Solenoids are electromagnets that are made out of a huge copper wire coil with an armature in the middle. The slug is drawn into the center of the coil as it is charged. This allows the solenoid to pull from only one end.

An LCD is an electrical display module that employs liquid crystals to generate a visible image. The primary advantages of utilizing this module are its low cost, ease of programming, animations, and the fact that there are no restrictions on displaying unique characters, special animations, and so on.

B. Fingerprint Authentication System

One of the most fundamental biometric traits is fingerprinting. Dactyloscopy is the field of study that deals with fingerprints. The papillary lines on the inside of human fingers are the subject of this study. Every person's papillary lines, as well as their form, course, and orientation, are unique. It is feasible to establish numerous basic patterns that assist to categorise all of the forms based on the shapes created by the papillary lines. Four patterns are used as a criterion for classifying each fingerprint. As seen in Fig. 2, Arch, loop, and whorl are three primary fingerprint pattern ridges. The following is an explanation for the three primary fingerprint pattern ridges:-

- Arch: The ridges enter from one side of the finger, ascend in the center to create an arc, and then leave from the other side.
- Loop: The ridges enter from one side of the finger, curve, and leave on the same side.
- Whorl: Ridges on the finger develop in a circular pattern around a central point. Ridges develop in a circular manner around a finger in the whorl pattern.

Fig. 2. Types of the fingerprint pattern [16]

C. Experimental Setup

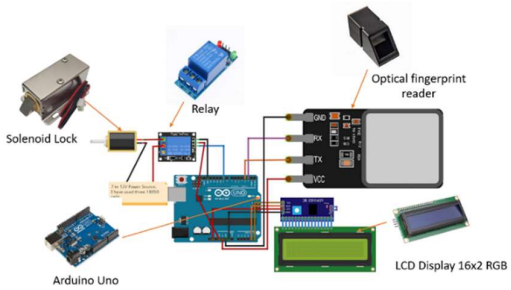
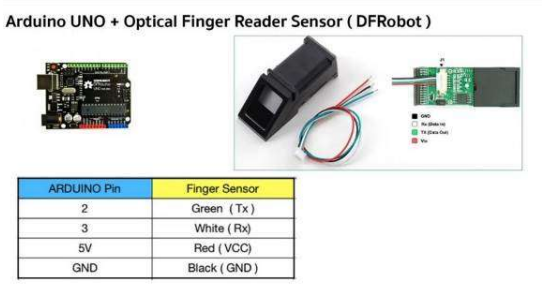


Fig. 3. Experimental setup for the proposed system

Fig. 3 presents the experimental setup for an Arduino Based Smart Fingerprint Authentication System for Key Security Locker. Based on Fig. 4, the optical fingerprint is as an input and is connected to the Arduino board. Pin 2 is assigned to the transmitter (Tx), whereas Pin 3 is assigned to the receiver (Rx). The Arduino Uno supplies 5v to power the fingerprint reader. Fig. 5 shows the connecting of Vcc to 3.3v, the LCD 16x2 is linked. Then, connect the Serial Clock (SCL) to pin A5 and the Serial Data (SDA) to pin A4.



ARDUINO Pin	Finger Sensor
2	Green (Tx)
3	White (Rx)
5V	Red (VCC)
GND	Black (GND)

Fig. 4. The connection between an Arduino board and an optical fingerprint reader

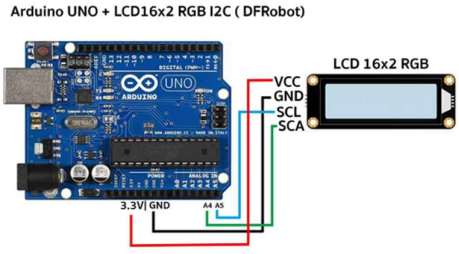


Fig. 5. Connection LCD 16x2 and Arduino board

Fig. 6 shows the connection between the Arduino board with the relay module and the solenoid lock. The relay module acts as an on/off switch. IN1 is connected to pin 9 and 5v is supplied to the relay module from the Arduino board. Besides, NO is connected to the solenoid lock-in anode polarity. The negative polarity of the solenoid lock and pin COM are both connected to the power source 12V.

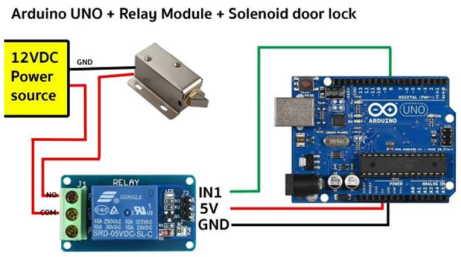


Fig. 6. The connection between an Arduino with a relay module, and a solenoid lock

Fig. 7 depicts the flow chart for this proposed system. When the user places a finger on the scanner, the fingerprint sensor illuminates the surface of the finger and records the minutiae using a charge-coupled device (CCD) with an 8 bit per dot resolution of 500 dpi (dots per inch) in grey-scale. The collected data is saved in a local database once it has been transformed into a digital signal. Every time a fingerprint is scanned, a new human minutia is captured. These new details will be compared to those in the database to determine if the individual is permitted or not.

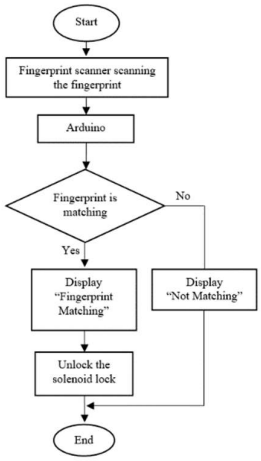


Fig. 7. Flow chart of the proposed system

D. Software Arduino (IDE)

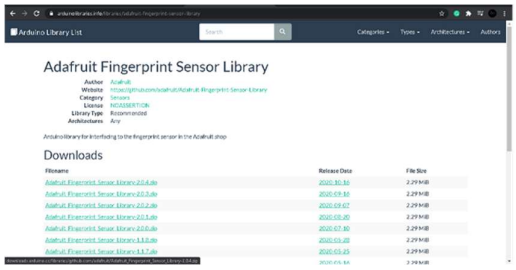


Fig. 8. Adafruit fingerprint library in Google

The Arduino Adafruit fingerprint library can be downloaded from the Google website as shown in Fig. 8. After downloading the library, copy and paste the Adafruit fingerprint library into the Arduino library. Fig. 9 shows the coding for Adafruit_Fingerprint.h while Fig. 10 shows the coding for the proposed system in the Arduino software.

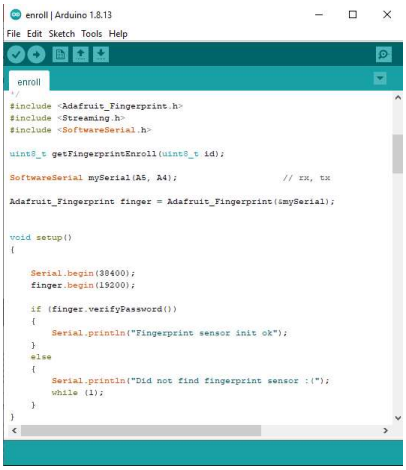


Fig. 9. Coding for Adafruit_Fingerprint.h

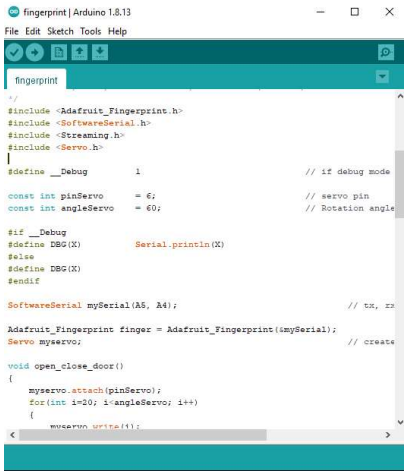


Fig. 10. Coding for Fingerprint

III. RESULTS AND DISCUSSION

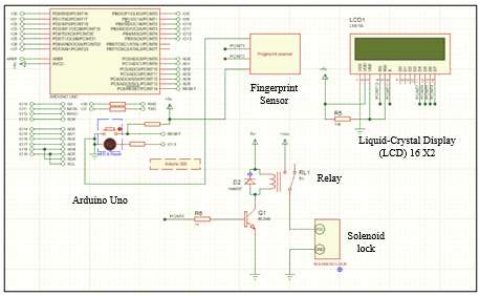


Fig. 11. Schematic design

The schematic diagram for an Arduino-based Smart Fingerprint Authentication System for Key Security Locker can be found in Fig. 11. The input voltage for Arduino Uno is 5V while the solenoid electric lock requires 12V. The Arduino Uno MCU board serves as the circuit's brain. It contains 14 digital I/O pins, six analog inputs, 32k flash memory, a 16MHz crystal oscillator, a USB connection, a power connector, an In-Circuit Serial Programming (ICSP) header, and a reset button, among other features. It can be programmed using Arduino Integrated Development Environment (IDE) software. The fingerprint sensor is an optical fingerprint scanner that also serves as an input. The user can store fingerprint data in the module and set it for identification in 1:1 or 1:N mode. The sensor's Tx and Rx pins are linked to Arduino digital pins 2 and 3 for serial communication. The LCD is used to display the output messages. As a result, a 5V Relay (RL1) is needed to operate the lock. The Normally Open (N/O) contacts of RL1 are linked to Ground through CON3 (GND). Connector CON3 is used to connect an electronic door-lock solenoid. It's an electromagnet with a large coil of copper wire in the center and an armature in the center. The slug is drawn into the center of the coil when it is electrified. The solenoid can now be moved to one end.

(a) Front view (b) Side view

Fig. 12. Front view and side view of the proposed system

Fig. 12 shows the front view and side view of an Arduino Based Smart Fingerprint Authentication System for Key Security Locker. The first step when accessing this Key Security Locker System, the user needs to place their fingerprint on the optical fingerprint scanner. The optical fingerprint scanner will be scan the fingerprint.

(a) Fingerprint scanner (b) Fingerprint matching

Fig. 13. Fingerprint matching

Based on Fig. 13, the fingerprint scanning event will capture a new humans minutiae. These new minutiae will be compared to those in the database to determine whether the person is authorized or non-authorized. If the fingerprint matches one in the database, the Liquid Crystal Display (LCD) will display "Fingerprint Match.". Then, the microcontroller will instruct relay and solenoid lock to unlock the locker door as shown in Fig. 14.

(a)

(b)

Fig. 14. When the fingerprint is matching, a solenoid lock will unlock the locker

If the fingerprint is not matched, the LCD will appear "Not Matching". Then, the locker door will remain locked as shown in Fig. 15.

Fig. 15. Not matching

Table I shows that an Arduino Based Smart Fingerprint Authentication System for Key Security Locker is a locking system that uses a fingerprint sensor module to authenticate the user's fingerprint. Arduino is used to power the fingerprint sensor module. The Fingerprint module determines whether or not a particular fingerprint is allowed. The locking system uses the user's fingerprint to open the system.

TABLE I. RESULTS FOR AN ARDUINO BASED SMART FINGERPRINT AUTHENTICATION SYSTEM FOR KEY SECURITY LOCKER

Finger-print	Type of Fingerprints	Matching/ Not Matching	Database	Key Security Locker Door
1	Tented Arch	Not Matching	No	Close
2	Central Pocket Loop	Matching	Yes	Open
3	Plain Left Loop	Matching	Yes	Open
4	Plain Loop	Not Matching	No	Close

Based on Table II, the common comparison is the Key Security Locker System using a fingerprint lock while product A still uses a traditional lock that uses a key. Besides, the Key Security Locker has a high level of security due to it using a fingerprint system that allows a valid fingerprint to access it. The Key Security Locker is more expensive than product A since it uses electronic components and coding to construct it. Furthermore, the Key Security Locker uses a power supply while a traditional lock does not. This locker has been developed with a more modern and stylish design.

TABLE II. COMPARISON OF PROPOSED SYSTEM WITH TRADITIONAL LOCK

Product	Product A	Proposed System
Type of lock	Traditional lock (using key)	Fingerprint lock
Security	Low-level security/easy to access	High-level security/difficult to access
Power Supply	Do not need supply	Need power supply
Design	Traditional look	Modern and stylish

An Arduino Based Smart Fingerprint Authentication System for Key Security Locker is designed to ensure the key storage is in a more organized and effective location. Fingerprints are unique to each person and cannot be lost or stolen, making them extremely accurate and dependable. This suggested device can safely store a large number of keys in one location. This technology recognizes authorized personal's unique fingerprints and allows them access.

IV. CONCLUSION

An Arduino-based Smart Fingerprint Authentication System for Key Security Lockers has been created, which offers improved security, efficiency, and user convenience in many cases. By using this innovative product, the keys can be stored in a more organized and secure location. Only authorized users can open the door of this key security locker to access the key insides of this locker. Thus, with biometric technologies like fingerprint scanning, authentication can be made more secure and convenient. Biometric technology's use will continue to expand in the future, and it will be employed in even more sectors that affect our daily lives.

REFERENCES

[1] H. Hassan, R. A. Bakar, and A. T. F. Mokhtar, "Face recognition based on auto-switching magnetic door lock system using microcontroller," in 2012 International Conference on System Engineering and Technology (ICSET), IEEE, 2012.

[2] Y. T. Park, P. Sthapit, and J.-Y. Pyun, "Smart digital door lock for the home automation," in TENCON 2009-2009 IEEE Region 10 Conference, IEEE, 2009.

[3] Keriya, F.R.B., "Development of IoT–based locking system," B.S. dissestation, Dept. Faculty of Electrical and Electronic Engineering (UTHM), Johor, Malaysia 2019.

[4] Z. Mumtaz, Z. Ilyas, A. Sohaib, S. Ullah, and H. A. Madni, "Design and implementation of user-friendly and low-cost multiple-application system for smart city using microcontrollers," arXiv preprint arXiv:2010.07016, 2020.

[5] Y. Motwani, S. Seth, D. Dixit, A. Bagubali, and R. Rajesh, "Multifactor door locking systems: A review," Materials Today: Proceedings, 2021.

[6] S. Goyal, P. Desai, and V. Swaminathan, "Multi-level security embedded with surveillance system," IEEE Sensors Journal, vol. 17, no. 22, pp. 7497-7501, 2017.

[7] S. Hossain, M. I. Ahmed, and M. N. Mostakim, "A prototype of automated vault locker solution for industrial application," in 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), IEEE, pp. 1-7, 2019.

[8] A. M. A. Bakry, and D. R. Rajaa, "Smart phone-Arduino based of smart door lock/unlock using RC4 stream cipher implemented in smart home," International Journal of Advanced Computer Technology, vol. 5, no. 5, pp. 14-18, 2016.

[9] G. K. Verma, and P. Tripathi, "A digital security system with door lock system using RFID technology," International Journal of Computer Applications, vol. 5, no. 11, pp. 6-8, 2010.

[10] N. Meenakshi, M. Monish, KJ. Dikshit, and S. Bharath, "Arduino based smart fingerprint authentication system," in 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), IEEE, pp. 1-7, 2019.

[11] T. Adiono, S. Fuada, S. F. Anindya, I. G. Purwanda, and M. Y. Fathany, "IoT-enabled door lock system," International Journal of Advanced Computer Science and Applications, vol. 10, no. 5, pp. 445-449, 2019.

[12] O. Doh, and I. Ha, "A digital door lock system for the internet of things with improved security and usability," Advanced Science and Technology Letters, vol. 109(Security, Reliability and Safety 2015), pp. 33-38, 2015.

[13] T. Tanjin, and S. Akter, "Design and implementation of Arduino based home security system," International Research Journal of Modernization in Engineering Technology and Science, vol. 3, pp. 1335-1338, 2018.

[14] H. S. Eldo, "Fingerprint based security system for ATM," International Research Journal of Engineering and Technology, vol. 6, pp. 850 – 854, 2019.

[15] F. Hidayanti, F. Rahmah, and A. Wiryawan, "Design of motorcycle security system with fingerprint sensor using arduino uno microcontroller," International Journal of Advanced Science and Technology, vol. 29, no. 5, pp. 4374-4391, 2020.

[16] S. B. Ahmed, and M. I. Razzak, "The minutiae based latent fingerprint recognition system: A comprehensive survey," Proceedings of the International Conference on Internet of things and Cloud Computing, 2016.