International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Automated Security Door System Using Fingerprint as Authentication for Access

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba
Department of Computer Science, Waziri Umaru Federal Polytechnic, Birnin Kebbi, Kebbi State, Nigeria
E-mail: {abduljedo, abafo22, suwaizay, musaibnabubakar}@gmail.com

Abstract— *Security with relation to people's lives and property continues to be a top worry in the modern era. It is a significant issue that presents difficulties for businesses, residences, governments, and people. In houses and hotels, standard security measures including the usage of keys, passwords, and cards are frequently utilized for authentication. Others include mechanical doors and lock codes. Due to staff using a single authentication access method that is not entirely dependable and trustworthy, these authentication approaches have been hacked, resulting in unlawful access that has resulted in losses such property theft and unauthorized admission by visitors into a hotel room. This study aims to advance existing methods by developing a new enhanced automated security door that uses fingerprint recognition to validate the fingerprint image before unlocking an electronic lock. At the conclusion of this study, a model and structure for an automated door that opens and closes using a security sensor without human guidance were established. The purposes of fingerprint verification are satisfied by comparing the information from the authorized fingerprint image with the received fingerprint image. The main elements used in this article to accomplish this goal are the Arduino Uno and ATmega2560 Board, Solenoid Lock, 12V Adapter, Fingerprint Sensor, and others.*

Keywords—*Arduino, Motor, Button, Biometry, Fingerprint, Sensor, Smart Door.*

I. INTRODUCTION

Automatic door openers are used all over the world. They can be found in a variety of places, including homes, retail malls, public buildings, airports, hospitals, and theaters. When a person approaches the door's entry, these systems open the door and close it once the individual has passed through. The sensor method, primarily controlled by circuits and motor make up the automated door opening system. The door is designed to be a protective system with a security device (Fingerprint Sensor) and operate automatically without human intervention. Burak et al (2015)

The automated data gathering used to identify people in support of their biological traits for authentication purposes is known as "biometrics. The two (2) categories of biometric technology are physiological (recognition of the face, fingerprint, hand, iris, and deoxyribonucleic acid) and behavioral (Keystroke, Voice, Signature Recognition). The person must be physically present for the biometric methodology to work. The fingers, face, or eyes of a person will be involved. Animals are, nevertheless, frequently recognized based on their skin patterns and biometric identification.

The first and oldest biometric technology, fingerprint recognition, has the potential to reduce costs for crucial and confirming the identity of someone in numerous applications. These days, everyone may perceive security as a serious issue when they are away from home or when they are occupied within the house. There is a chance that someone will attempt to open the door or any locked secret locker during these activities. One of th first problems when it comes to security systems is the inability to manually provide security for backdoor items. An alternative resolution with greater reliability and atomized security can be found as an alternative. These days, everything can be accessible with the aid of technology and may be filled with any necessary information. Correct security is needed in order to stop this precarious situation. These methods are highly unreliable because it is simple to steal valid identification and identification cards may disappear.

The advantage of fingerprint recognition is that it requires a lot of work to trick it and device of storing the fingerprints takes up less space in the information. Victimization of the fingerprint-based door unlocking system Security, forensics, and human identification are all aided by Arduino. Underneath the system's operation is a simple formula matching method. Therefore, only authorized users will have access to the door or locker using this manner. This study models an automatic door with a fingerprint sensor acting as the security and chooses the optimal fingerprint-based components.

II. RELATED WORK

The design and execution of a fingerprint-based lock system can be altered to meet the needs of the user, according to Ganesh Sahithi Murru, Chetan Kakollu, Ashok Kumar Kenguva, and P. Surya Chandra (2020). Comparing this lock protection mechanism to older lock systems on the market, it is more effective. It is decided to use a system that offers high security and encompasses a high rate of accuracy. In our country, both private and public organizations are heavily involved in security-related issues, and many businesses are interested in utilizing various forms of protection mechanisms. However, the available system has an extremely expensive installation cost. Many small businesses are unwilling to buy such systems due to the exorbitant cost.

We tend to plan to design a system that is inexpensive to a very large, for a very small businesses, and homes while taking installation costs into consideration of the users who accessed the lock and send an alert notification to the mobile device in case of 3 failure attempts. With this approach, a system that

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

provides users with security is far more practical, efficient, and dependable. The system was able to read and match the sensor's limits when tested with an oily or muddy finger, but he failed. In normal or dry conditions, the sensor recognizes saved prints without any distortions. As a result, during testing, the planned system had a 95 percent success rate.

A model of a fingerprint-controlled door system with multi-access authentication based on the Internet of Things (IoT) was presented by Akanbi C. O., I. K. Ogundoyin, J. O. Akintola, and K. Ameenah in 2020. His system architecture shows how various components interact via the Internet of Things (IoT). The Circuit Diagram for the system was designed to detail how different modules connect to one another. Using the design implementation mentioned, customer fingerprint templates received during in-person or online room reservations, as well as fingerprint templates taken at each room's door, are saved on the web server. The prototype system only unlocks the door if the fingerprints on both templates matched.

Biometric Fingerprint and Iris Recognition Technology for Smart Homes is a topic of research according to Shoewu, Olaniyi, and Lawson (2021). A method with multiple biometrics was employed to guarantee consistency. A database template was created and saved using the users' fingerprint and iris data. When performing authentication, iris and fingerprint recognition technologies (FRT and IRT) receive and compare biometric information with database material. Any inconsistency in the data will prevent permission. The system's inability to accommodate users with impairments continues to be a serious flaw despite the multiple security levels.

Real-Time Smart Door System for Home Security, published by Burak, Tolga, and Huseyin in 2015, is currently accessible. The system uses the Raspberry Pi and video technological breakthroughs as a security and safety tool to recognize and see visitors to the residence. The study makes use of two different technologies (Video and Smart Phone). The phone server was utilized as a voice communication tool, and the video was used to keep a real-time eye on the front door. The method used in the study offers customers a variety of benefits, such as the ability to stream events happening behind the door and to see who is at the door without having to open it. The enormous expense of actual implementation in the real world is the system's basic shortcoming.

According to KHIN EI EI KHINE (2018), said the majority of the digital IC components are housed in the PIC microcontroller in. Switches and sensors for sensing are examples of input devices. The system outputs are the LCD display and motor control. The circuit diagram is now simple to understand. You only need a fundamental knowledge of microcontrollers and programming to build this system. The door can be opened and closed using a variety of parts, including a motor and a solenoid valve. In this thesis work, a DC motor driven by an L293 motor driver is used. The L293 can control bi-directionally for DC motor drives. Switches that detect edges turn on and off motors. A software program can control the forward, reverse, and stop functions of a motor. On the Liquid Crystal Display (LCD) display screen, the output data is displayed. Glass is used to make a single slide door. The size of the door is 2 m2.5 m. The 100 W DC motor is used to open and close the door. These motors are controlled by the PIC 16F877 microcontroller. The system's overall functionality and performance are impacted by the individual entering through the door and how near they are to the entrance. Although the door is intended to open automatically, forcing it to do so in the event of a power outage could damage the mechanical control system of the device.

The majority of biometric data is gathered using fingerprint, palm, and DNA analyzers, according to Hteik HtarLwin, AungSoe Khaing, and Hla MyoTun (2015). During the data collecting procedure, the needed equipment must come into contact with the target items. The benefit of this technique is that facial recognition hardware is not necessary. Automatic face detection is achieved via face detection technology, and face recognition is completed without the usage of any hardware. Technology for facial recognition is used in automated door entry. How to detect is demonstrated.
Automatic face detection and recognition is performed by Matlab, a PC program. The door access system is controlled by a microcontroller utilizing information from a computer (PC).

The door will be opened right away after confirmation and after the person has been verified. The door automatically shuts after two seconds. In actuality, 2 seconds is insufficient to penetrate a person. Therefore, a longer length should be selected for real-time circumstances. The position of a face in a picture is determined using the Viola-Jones face detection method. This detection method has limitations in terms of head angle because it can only accurately recognize frontal view face images. The Principal Component Analysis technique is used to identify faces by extracting the key features of facial photos. Due to the PCA technique's ability to minimize the size of the dataset, this system can detect and identify an image in one second. As a result, this technology can be applied to automate the verification of individuals. Therefore, without the requirement for security guards or excessive time spent, this method can be used for automatic person verification to increase door security for strangers.

It is one of the most typical concerns, according to Hashem Alnabhi, Yahya Al-Naamani, Mohammed Al-Madhehagi, and Mohammed Alhamzi (2020). We are all looking for workable solutions and concepts to protect our valuables and private information from burglars. Unauthorized people or thieves could try to break down the door when no one is around for destructive purposes; as a result, this article offers a variety of security solutions for that issue, which is the core contribution of our work. The introduction of an alert system and a GSM module for sending SMS messages to registered users. (Responsible Person) uses a password keypad following fingerprint sensing for enhanced security, together with a web camera that captures any lockpick attempts. A real-world scenario was used to test the proposed security mechanism, and the results were promising. A webcam, a password system, and other added security measures set the system apart and boost its competitiveness. Future work on this topic will likely cover a wide range of topics, including the addition of many additional security tools like iris scanners for visual identification, fire sensors linked to alarms, and artificial intelligence-enhanced systems that can speed up the process of identifying a person by

using face recognition technology with a database of well-known burglars.

Amuda F.A., Tennyson D.I. claim that law enforcement has been using fingerprint identification for over a century (2017). In order to unlock an electronic lock, a fingerprint locker system with a microcontroller verifies the fingerprint image using a fingerprint recognition system. The development of a fingerprint verification system using Arduino 1.6.3 is the main goal of this study. The information from the accepted fingerprint image is compared to the information from the incoming fingerprint image to complete the verification. The information from the entering fingerprint image will be retrieved and filtered using the extraction and filtering techniques. The information from the permitted fingerprint image and the arriving fingerprint image will next be compared. In this study, the fingerprint module was instructed to find and learn new fingerprints. if the fingerprint image received is authentic or not. The use of fingerprints for personal verification, such as acquiring access to a computer, network, ATM, car, or home, is much more widespread. The goal of the project is to create a fingerprint lock that can be utilized for vaults, doors, and other electronic locking systems. The research goal would be considered to have been achieved once the device was built and found to be operating as intended, especially given the relatively modest cost of the components used in its construction. The method can be utilized as a security lock as well.

The microcontroller-based system for securing user transactions, providing security for the locker system, and passport verification using a finger print scanner was designed using a step-by-step process, according to Kodandaramaiah, D. ArunTeja, and Y. S. Raghu Ramarao, I. Adiyta (2019). In all the three ways, the outcome of ensuring security is extremely trustworthy. By utilizing finger print biometrics as an authentication method, the system has successfully solved some of the drawbacks of current technologies. The project's goal is to create a fingerprint lock system that can be applied to doors, other electronic locking systems, and vaults in addition to being used to lock and open doors. The research objective can be regarded to have been met when the device was realized and found to be. Given the modest cost of the materials used in its construction, it is operating effectively in accordance with its design parameters. The technique can also be used as a security lock.

The fingerprint-based security door control system employed in this study, according to Joseph O. Odiete and Abayomi O. Agbeyangi (2017), enables electronic door manipulation. It gets around the issues with relying on human security. With minimal to no human involvement, it opens and closes the door, increasing efficiency and security. When compared to other modern systems, this method is more effective because of how quickly it can identify users. Image capture, signature extraction, and storage are the three parts in the enrolment process. It provides a summary of the registration numbers. The number of administrators and the list of users with access to the security door system log in, navigate through the application pages, and finally log out

III. METHODOLOGY

A locking door, an interface control system, components, and a C-based control application are just a few of the subsystems that make up the creation of a fingerprint-based door control system. The created control program application, whose function is based on sensing the matched fingerprint with the database template, controls the interface control circuit, while the interfacing control circuit controls the door lock for opening and closing activities.

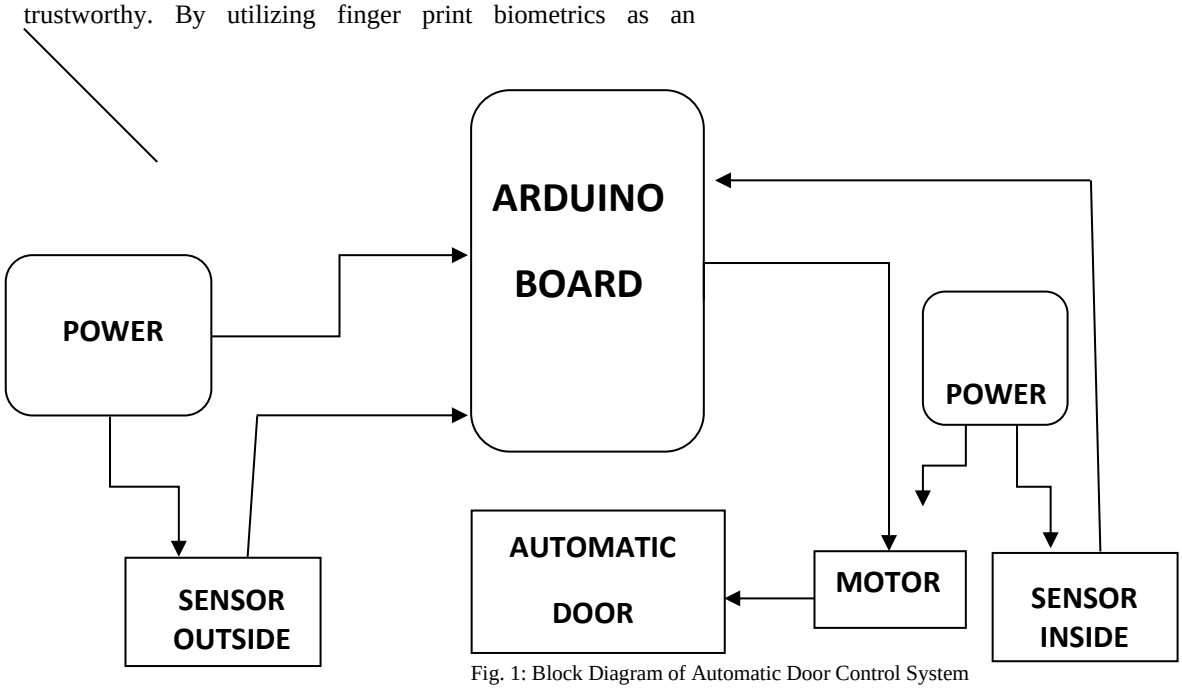

Fig. 1: Block Diagram of Automatic Door Control System

In the overall process flow, computers are utilized primarily for two tasks: sending the source code and the registration fingerprint template to the Arduino. When the authorized user places his or her finger on the device for identification, the

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

fingerprint device (which serves as an input device) is used to capture the template image and send it to the computer (PC). All of the templates are then assigned to the arduino controller for storage in the database.

Only when the fingerprint frames obtained match those in the database prior to accessing the entrance door will the prototype activate the sensor, motor, and open the door.

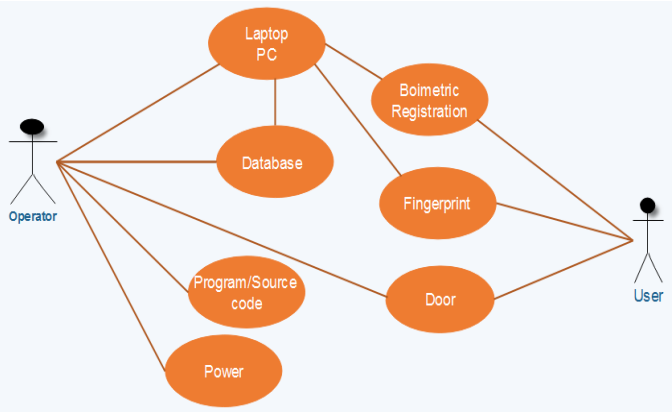

Fig. 2: UML Use Case for Interactive Access

The diagram above showed what the operator should have access to, including laptops, PCs, databases, biometric registration and fingerprint (using a laptop or database to store a fingerprint template), program/source codes, power, and the door since the operator acts as the gatekeeper for all door-related processes. The door, fingerprint device, and biometric registration should be accessible to the user. A user or intrusive party must not have access to the laptop computer's power supply, software, source codes, or database for security reasons (storage).

Interaction between Hardware and Software

The interface control system for the development is shown in Figure 2. The stepwise procedures in the system interaction are:

1. *Finger Print Acquisition*: The acquisition of finger print was obtained from the finger print sensor hardware and few information about authorized person were also collected through the soft ware interface,
2. *Feature Extraction*: Features were extracted from each of the individual finger print by using a feature extraction algorithm,
3. *Template Generator*: A template was generated for each of the features extracted and finally stored.
4. *Stored Templates*: The extracted features were stored as a template in the system database.
5. *Matching*: A matching algorithm was applied by the control program

Evaluation: The performance of the system was evaluated based on time of recognition.

The study's two major components, hardware and software, were combined using an interface technique.

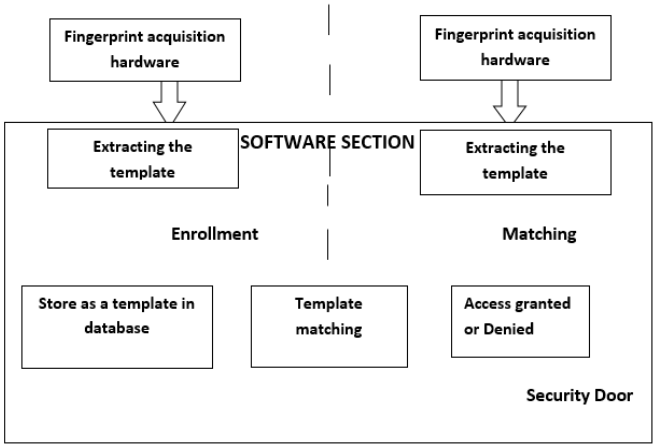

Fig. 3: The System Development framework

Software Part

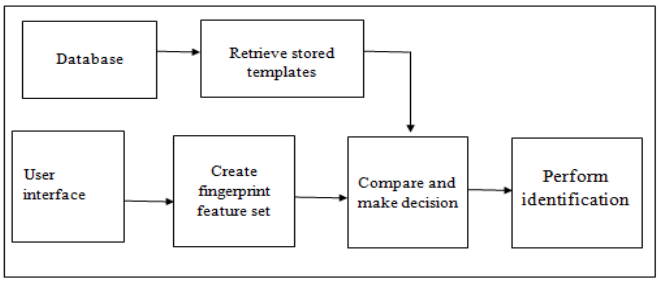

Fig. 4: The System Software Identification Process

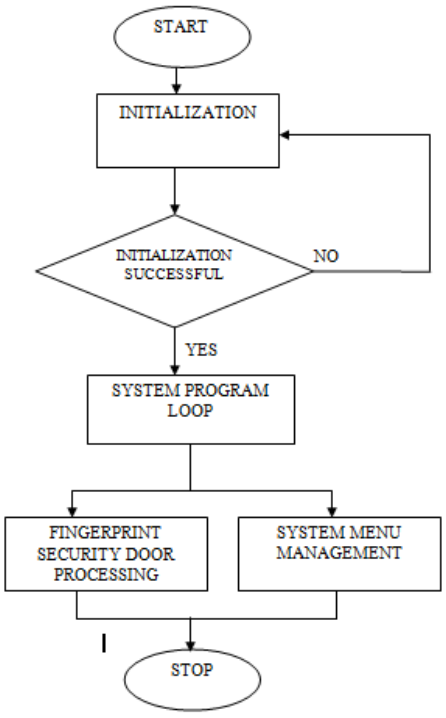

Fig. 4a: System Control Program Process

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

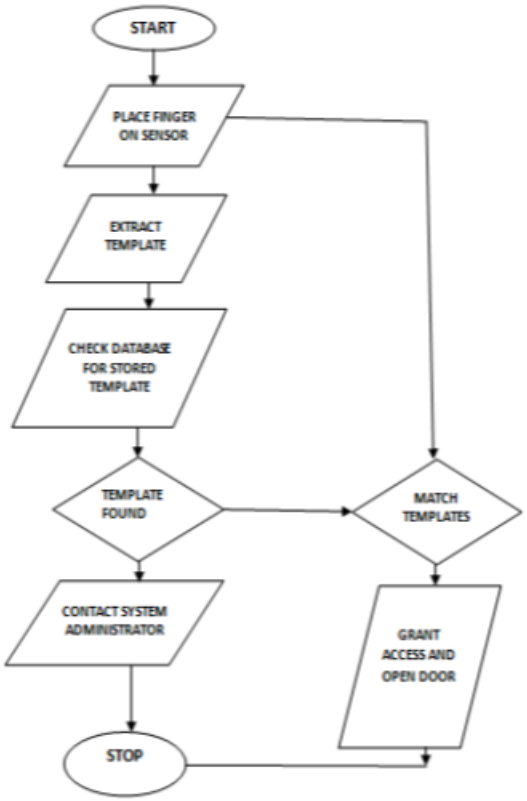

Fig. 4b: Matching and Verification Process

Characteristic

Microcontroller Board	ATmega2560
Operating Voltage	5V
Input Voltage (Recommended)	7-12V
Input Voltage (limits)	6-20V
Digital I/O Pins	54 (of which 14 provides PWM output)
Analog Input Pins	16
DC Current per I/P Pin	40mA
DC Current for 3.3V Pin	50mA
Flash Memory	256 KB of which 8 KB used by boot loader
SRAM	8 KB
EEPROM	4 KB
Clock Speed	16 MHz

Components Part Overview

The Arduino Mega 2560 microcontroller board was built around the ATmega2560 processor. The board has 16 analog inputs, 4 hardware serial ports (UARTs), a 16 MHz crystal oscillator, 54 digital input/output pins (14 of which can be utilized as PWM outputs), a USB connector, a power jack, an ICSP HEADER, and a RESWT BUTTON. It includes everything you need to support the microcontroller; all you need to do is connect it to a computer using a USB cable or power it using an Arduino Duemilanove or Diecimili shield. Board for Arduino Mega (2560).

Arduino is an electrical platform that is open-source, free, and has basic hardware and software. An LED can be turned on, a motor can be started, and anything can be published online using Arduino boards, which can read inputs like a light on a sensor, a finger on a button, or a tweet from Twitter. The microcontroller board can be programmed with instructions to tell it what to do. Use the Arduino software (IDE) and the writing-based Arduino programming language to accomplish this (which is based on processing). Arduino has been the brain of thousands of projects throughout the years, from little domestic products to massive scientific instruments. Around this open source platform, a global community of makers, students, hobbyists, artists, programmers, and professionals have gathered, and their contributions have built up to an astonishing amount of accessible knowledge that might be of enormous benefit to both beginners and experts. Software called Arduino makes it simple to combine code and hardware. Placing a finger on a sensor or pressing a button, turning on a diode, or sending a message, these boards are used to browse inputs. The microcontroller can be programmed with instructions that tell the board how to operate. To include the instructions, which have a number of steps or stages, we can use the Arduino IDE and Artificial Language.

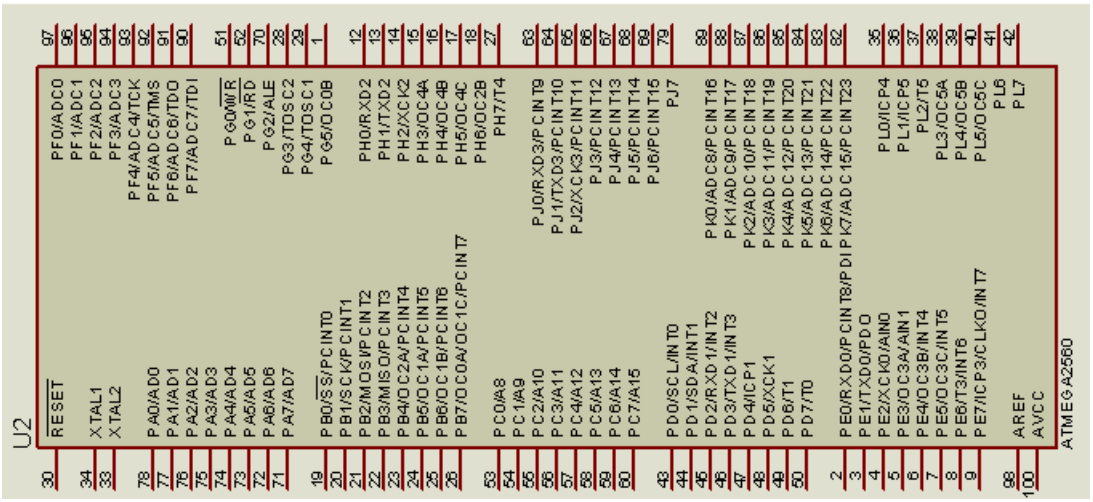

Fig. 5: Schematic Arduino Mega (2560) Board

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

An application that enables the creation of electronic circuits is called the Arduino IDE (Integrated Development Environment).
Information is kept in a wording console, a technical bar with a number of switches for related tasks, and a number of lists. Genuine Arduino hardware is utilized to share data and transmit programs. A fundamental tool for rapid prototyping has been created by the Ivrea Interaction Style Institute. It is currently diversifying its supply in order to react to new wants and issues. Since each board is an ASCII text file, users can modify it in various ways to suit their individual requirements.
As a result of its extensive usage, it is growing in popularity globally.

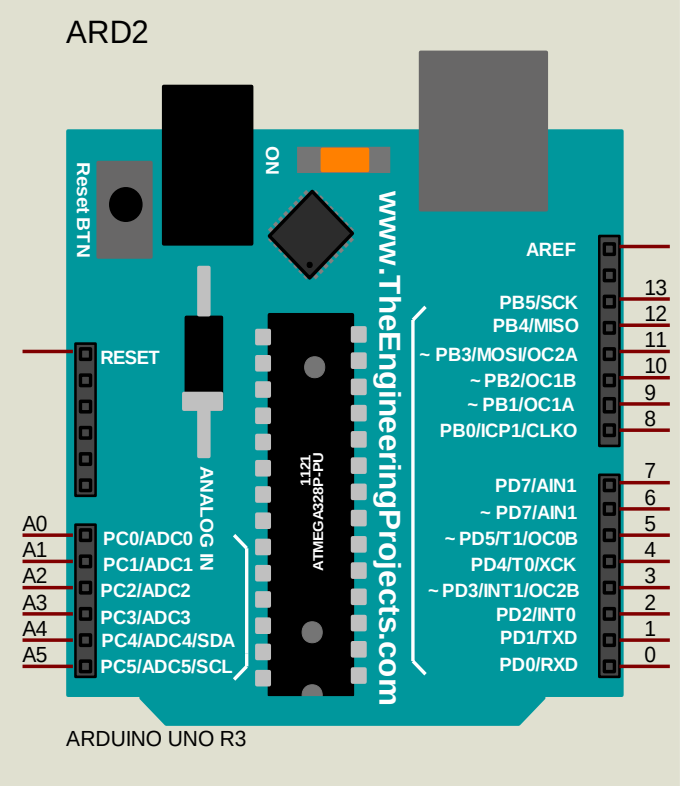

Fig. 6: Arduino UNO (R3) Semi-Board

SM630 Fingerprint Sensor Module

A device that electronically records a digital image of the fingerprint pattern is known as a fingerprint sensor module. This is required in order to compare, store, and match fingerprints. A template (a set of traits from the person retrieved from the captured image, or live scan), is produced and used for digital authentication. The Digital Signal Processor (DSP), ROM, and memory of this sensor are all present. The biometric fingerprint sensor, which includes a DSP controller for simple interface with an Arduino pin, is the key component for verifying fingerprints. The most recent item from Miaxis Biometrics Company Limited is a background highlight optical fingerprint verification module, model number SM630. It consists of a flash memory, a powerful DSP processor, and an optical fingerprint sensor. Among other things, it provides fingerprint login, deletion, verification, upload, and download capabilities. The SM630 stands out from comparable products in the following ways:

The optical fingerprint gathering device, the module hardware, and the fingerprint algorithm were all created by the firm and are considered to be its intellectual property.

High Adaptation for Fingerprints when reading fingerprint images, it has a self-adaptive parameter adjustment mechanism that improves imaging quality for both dry and wet fingertips. A bigger audience can use it.

The overall cost is significantly decreased by using Miaxis' optical fingerprint collection technique in the Low Cost Module. The picture generation theory of the optical fingerprint gathering device served as the inspiration for the SM630 module algorithm. It offers excellent correction and tolerance for crooked and subpar fingerprints. The user does not have to be an expert in fingerprint recognition. Users can easily build effective fingerprint verification application systems based on the wide variety of application systems available.

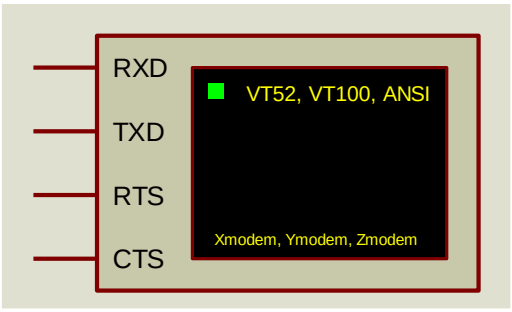

Fig. 7: Schematic Fingerprint Sensor

Solenoid Lock

A solenoid locks a door or other object using electromagnetic forces to operate the lock. When locked, the solenoid's coil stretches inside the safety mechanism, making it impossible to forcefully unlock the device. The user's fingerprints are serially verified by the Arduino. If the user's fingerprint matches a stored or memorized fingerprint, the solenoid door lock automatically unlocks.

Fingerprinting by unauthorized individuals will bar access.

Fig. 8: Solenoid Lock

Tip 122 Transistor

A Darlington pair NPN transistor is the Tip 122 transistor. It acts somewhat like a conventional NPN semiconductor device with three pin-outs for base, collector, and emitter, but because it's a Darlington pair combined, it has a good collector

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

current rating of about 5A and a gain of about 1000. It can drive high loads because it can withstand up to 100V across its collector-emitter.

Power

The Arduino Mega and Arduino UNO are typically powered by USB connections or external power sources, but for this project, Proteus (Schematic) software simulation was used to build both boards with an internal powered supply. In reality, the power source is chosen at random. External (non-USB) power can be supplied by a battery or an AC-to-DC adaptor (wall wart). The adapter can be connected to the board's power port using a 2.1mm center-positive socket. Battery leads can be inserted into the Gnd and Vin pin headers of the POWER connection. An external supply ranging from 6 to 20 volts can power the board. However, if supplied with less than 7V, the 5V pin might output less than five volts. If pin delivers less than five volts, the board can become unstable. If you utilize more over 12V, the voltage regulator could overheat and obliterate the circuit board. The recommended voltage range is between 7 and 12 volts. Because it does not have the FTDI USB-to-Serial Driver chip, the Mega2560 differs from the earlier boards in this regard. Instead, it makes use of a coded Atmega8U2 already coded to work as a USB-to-serial converter.

Fig. 9: Schematic Power

The Power Pins Description

+VIN:- This is the input voltage when the Arduino board is powered by an external source (instead of the USB connector or another source of regulated power). When using the power jack to deliver electricity, this pin can be utilized to supply voltage or to acquire access.

+5V: A regulated power source powers the microcontroller and other components on the board. This may come from the VIN, a built-in regulator, USB, or another 5V source.

+3V3: A 3.3-volt supply is produced by the on-board regulator. A 50 milliampere maximum current draw is allowed (MA). Ground-connected pins are designated as GND.

Transistor

In this research work, a transistor is employed as a semiconductor device that amplifies or switches electrical and electronic impulses. The most crucial parts of contemporary electronics are transistors.

LCD Display

A flat-panel display or other optical device that is electronically operated and uses liquid crystals to modulate light is known as a liquid-crystal display (LCD). Liquid crystals don't produce light directly; instead, they produce color or monochromatic images using a backlight or reflector. LCDs can display fixed visuals with limited information content that can be shown or hidden, such as current text, numerals, and seven-segment displays, or arbitrary graphics (as in a general-purpose computer display) (as in a digital clock). They both employ the same fundamental technology, with the distinction that some displays use larger parts and some displays use random images made up of a huge number of tiny pixels. LCDs can be either normally on (positive) or off, depending on the polarizer configuration (negative). For instance, a character positive LCD with a backlight will have black lettering on a background that matches the color of the backlight, but a character negative LCD will have a black background and letters that match the backlight. Optical filters are used to produce white and blue LCDs their distinct appearance.

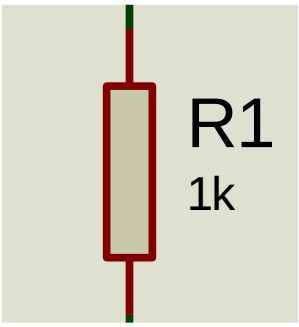

Fig. 10: Schematic Resistor

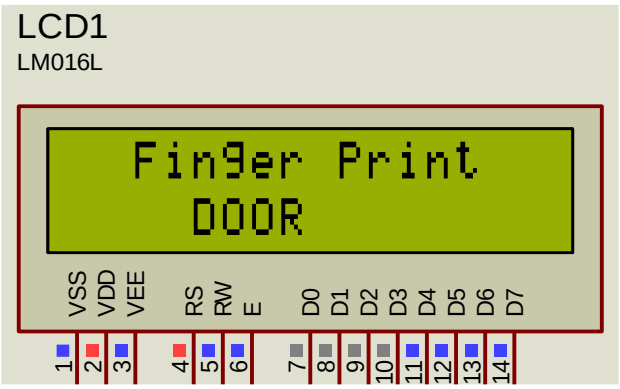

Fig. 11: Schematic LCD Display (LM016L)

Button SPST

The SPST button can be used in a variety of ways depending on the programmer's instructions. It can be used to represent or act as a button with digit numbers to replicate security password keys to open and lock, or it can be used as a button to initiate or stop an event. This project uses six (6) pushbutton keys (6-Keys) to perform the duties of adding and deleting fingerprints.

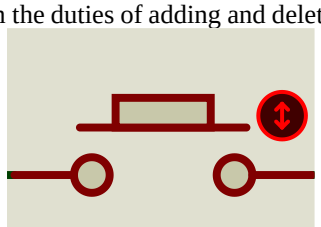

Fig. 12: Schematic Button (LM016L)

Memory

The ATmega2560 has 256 KB of flash memory, 8 KB of which are needed for the boot loader, 8 KB of SRAM, and 4

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

KB of EEPROM for storing code (read and writeable using the EEPROM library). Athlon 328.

Input and Output

Each of the 54 digital pins on the Mega can be used as an input or output thanks to the pin Mode(), digital Write(), and digital Read() routines. They operate at 5 volts. Each pin has a 20–50 k Ohm internal pull-up resistor with a maximum current capacity of 40 mA. (By default unconnected). For instance, several pins have unique uses:

Power is connected to VDD, resistor and ground are connected to VEE, RW, and VSS of the Arduino Mega2560, and Key (Push button) interface connection. LCD connections are D4-PD6, D5-PD2, D6-PD4, D7-PD3, E-PD7, and RS-PB0. Key interface ground-OUT(PIR)-A0 (Arduino) is connected to key interface ground-Key1 PC0 (OK), Key2 PC1 (up), Key3 PC2 (down), Key4 PC3 (cancel), Key5 PC4 (Add Finger), and Key6 PC5 (Delete Finger) with respect to ground connected at the other end pin, and Matching push button is connected to PB3 (Relay) of the Arduino Mega2560. PIR is connected to the second LCD display, OUT- A0, OUT- button, VCC-ground, Testpin -PL5, and GMD-ground. RS-13, E-12, D4-11, D5-10, D6-9, D7-8, resistor and ground are connected to VSS and RW, VEE-resistor 10k and power, VDD-VSS and VS, and 162 LCD is configured in 4-bit mode (L293D). Push-pull driver L293D is connected to IN1-1, IN2-0, VSS, VS, LCD VDD, OUT1 and OUT2 motor pins, and GND, ground. RXD-PE1 and TXD-PE0 are connected to the fingerprint sensor.

Servo Motor

An actuator that can precisely control angular or linear position, velocity, and acceleration is a servomotor. It is made up of a position feedback sensor and a suitable motor. Additionally, a sophisticated controller is required, which is typically a separate module made just for servomotors. It is not a specific type of motor, even though the term "servo motor" is frequently used to describe a motor suitable for use in a closed-loop control system.

Early transistor radios frequently used the nine-volt battery, also referred to as a 9-volt battery. It has a rounded rectangular prism shape, a polarized snap connector on top, and rounded edges. Clocks, smoke alarms, and walkie-talkies are all instances of this kind. Common nine-volt battery forms include primary carbon-zinc and alkaline chemistry, primary lithium iron disulfide, and rechargeable nickel-cadmium, nickel-metal hydride, and lithium-ion batteries. These particular mercury-oxide batteries haven't been produced in a while because of the mercury they contain. Some names for this format include NEDA 1604, IEC 6F22 (for zinc-carbon), or MN1604 6LR61. No matter the chemistry, the size is commonly referred to as PP3; nevertheless, this nomenclature was initially solely used for the size, carbon-zinc, or in some countries, E or E-block.

Battery

A common size of battery used in early transistor radios is the nine-volt battery, commonly referred to as a 9-volt battery. It has rounded sides, a rectangular prism shape, and a polarized snap connector on top. This kind is employed by smoke alarms, walkie-talkies, and clocks. Primary lithium iron disulfide, primary carbon-zinc, and alkaline chemistry, as well as rechargeable nickel-cadmium, nickel-metal hydride, and lithium-ion batteries, all use the nine-volt battery configuration. Despite being once widely used, this kind of mercury-oxide battery is no longer produced due to its high mercury concentration. This format has the designations NEDA 1604, IEC 6F22 (for zinc-carbon), or MN1604 6LR61.No of the chemistry, the size is commonly referred to as PP3.

Fig. 13: Battery

LED

A semiconductor light source called a light-emitting diode (LED) produces light when current passes through it. Recombining electrons and electron holes in the semiconductor results in the release of energy in the form of photons. Electroluminescence is the name of this phenomenon. The energy needed for electrons to bridge the semiconductor's band gap determines the color of the light, which corresponds to the energy of the photons. By layering numerous light-emitting phosphors on a semiconductor chip, white light can be produced.

Fig. 14: LED

Jumper Wire

A jumper wire is an electrical wire, or a group of them in a cable, with a connector or pin at each end that is typically used to connect, internally or with other machinery or components, the parts of a breadboard or other prototype or test circuit without soldering.

Fig 15: Jumper Wire

PIR Sensor

An electronic sensor known as a PIR sensor (Passive Infrared Sensor) monitors the infrared (IR) light emitted by objects in its range of vision. They are most frequently discovered in PIR-equipped motion detectors. PIR sensors are frequently utilized in autonomous lighting and security alarm

systems. PIR sensors generally detect movement but do not identify the object or person that moved. This requires a sensor that can image infrared light. The abbreviation "PIR" or "PID," which stands for "passive infrared detector," is frequently used to refer to PIR sensors. PIR devices are referred to as "passive" because they don't release energy in order to detect things. Only infrared radiation (radiant heat) that is emitted or reflected by objects can be detected by them.

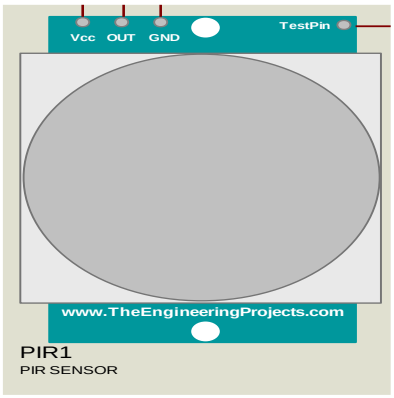

Fig. 16: Schematic PIR Sensor

DC Motor

A DC motor is any rotating electric motor that converts direct current electrical energy into mechanical energy. The most prevalent forms of force are produced by magnetic fields. Nearly all DC motors have an inbuilt electromechanical or electronic device that periodically reverses the current flow in a particular area of the motor. A brushed electric motor runs on a two-pole rotor (armature) and a permanent magnet stator.

The letters "N" and "S" stand for polarities on the inside and outside axis faces of the magnets, respectively. Where the DC current is applied to the commutator, which feeds the armature coils, is shown by the + and - marks.

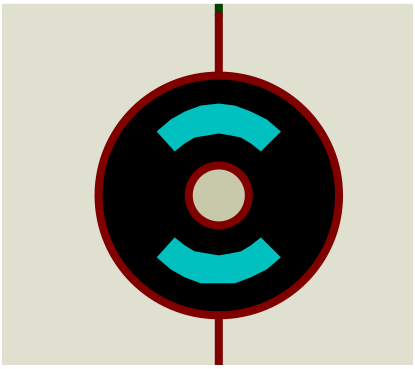
Fig. 17: Schematic DC Motor

POT Meter

A potentiometer is a three-terminal resistor with a sliding or rotating contact that creates a variable voltage divider. If only one end and the wiper are connected to the terminals, it can be utilized as a variable resistor or rheostat. The element implements the same principle as the potentiometer, a measurement tool used to measure electric potential (voltage). Electrical devices, such as volume controls for audio equipment, are frequently controlled by potentiometers. Potentiometers that are under the control of a mechanism, for instance, can be used as position transducers in a joystick.


Fig. 18: POT Meter

Software Description

Numerous software programs, including Keilu Vision5, Microchip Studio for AVR (SAM Devices), Arduino, and others, are open source. A programmer can use any of these software packages to accomplish the desired task (for programming, writing source code instructions), but each one has its own Integrated Development Environment, coding style, toolbar features, library, etc. Arduino was utilized in this project since it is more accessible to more programmers.

Arduino (IDE)

The free and open-source Arduino IDE makes it simple to write code and upload it to the board of your choice. Support for Windows, Mac OS X, and Linux is available.

The environment is created using open-source software like Processing and is written in C. The Arduino integrated Development Environment, or Arduino software, comes with a text editor for writing code, a message box, a text console, a toolbar with buttons for common functions, and a number of menus (IDE). It connects to the Arduino and Genuine hardware in order to upload the software and communicate with them.

IV. Results Presentation And Analysis

Introduction

Software testing is the process of examining the artifact and behavior of the software under test utilizing validation and verification.

In addition to software testing, the methods for debugging, identifying, validating, and resolving faults in the code are also necessary for a successful run of the program. The program is then tested again to see if it meets the criteria for attaining the goal.

Software Testing

When testing software, validation and verification are used to investigate the software's behavior and artifacts.

Along with software testing, other methods include debugging, finding, validating, and resolving mistakes in the code for a successful run of the program, as well as retesting the program to determine whether it meets the criteria for attaining the goal.

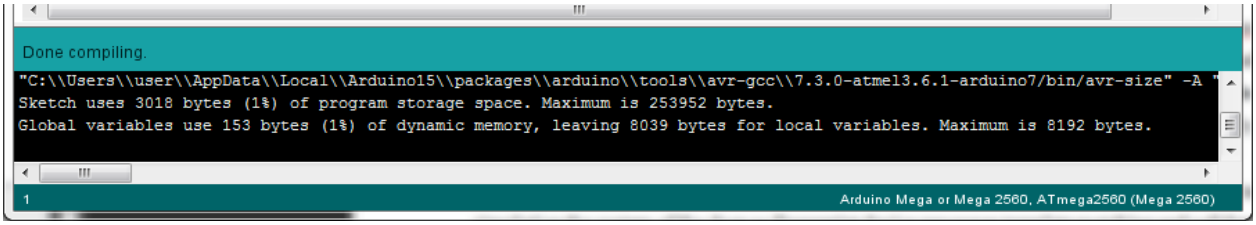

Fig. 19: HEX Compilation of Source Code

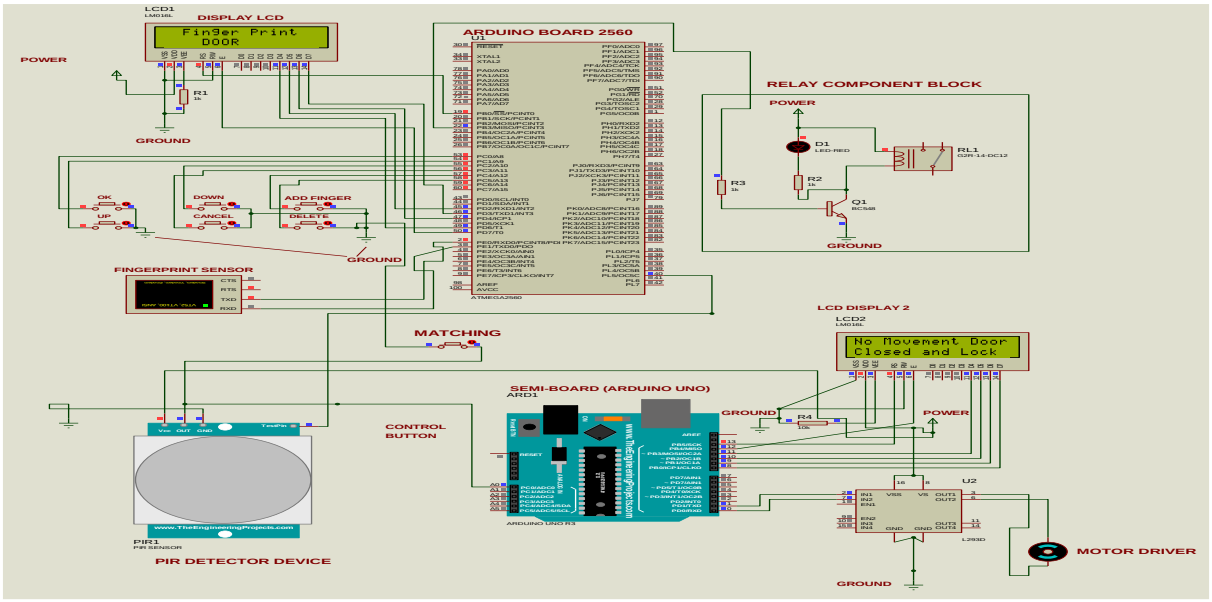

Fig. 20: Complete Shematic Circuit Diagram

Proteus software was used to simulate the system of the door as fingerprint device processes template matching and validates it before activating the sensor, after the sensor is active it sends signal to the motor, so it rotates clockwise for opening the door and pauses for 2 minutes (delay), and motor rotates anticlockwise for closing the door. Board does not accept any other file format other than HEX file (board supervise, controls all activities according to instruction). Due to the lack of a database, the demonstration of how the door opens and closes and how to add or remove a fingerprint module was not entirely successful in this study.

Algorithm:

1. Start/Power on state
2. Display on screen “Place Finger”3. Poll for Keys and Finger Search
4. Display on screen “Entry Successful” and Relay on for delay
    1. “Time out”
    2. “Process Failed”
5. Add Finger
    1. Display on screen “Add Finger” “Place Finger”
    2. “Time out”
    3. “Process Failed”
    4. “Entry Successful” “ID=??”
6. Delete Finger
    1. Display “Select ID”
    2. Use UP/Down Keys
    3. OK key to delete
    4. “ID=?? Deleted”

The above figure 20 was the screenshot of the full complete circuit dragram that was captured during the running time simulation in Protues 8 Professional.

Registration

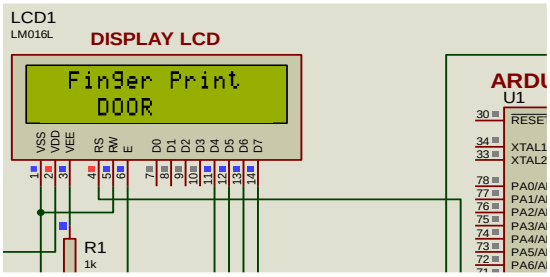

Fig. 20(a): Fingerprint Door

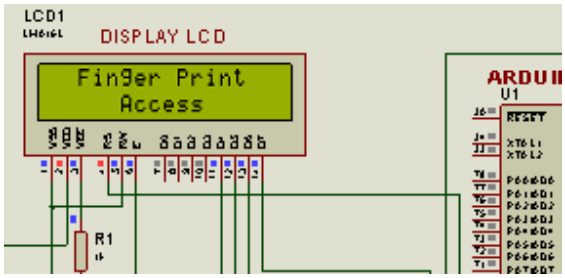

Fig. 20(b): Fingerprint Access

Fig 20(a) Is the first statement display by the lcd (Welcome Message) for the period of 1munite. Fig 20(b) After 1munite

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, “Automated Security Door System Using Fingerprint as Authentication for Access,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

(delay) then you can push the ADD FINGERPRINT button follow by the UP by the push button and the lcd will display Fingerprint Access (adding of fingerprint is ready)

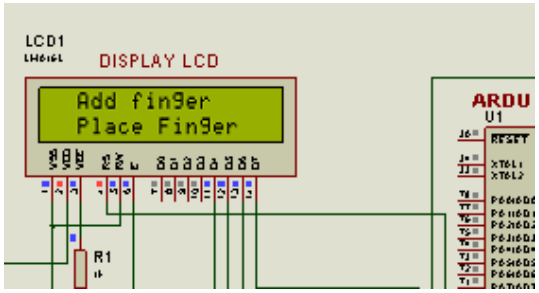

Fig. 20(c): Adding fingerprint template

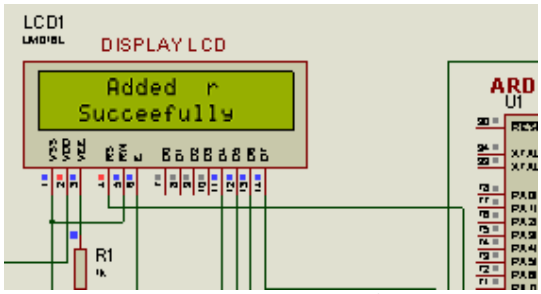

Fig. 20(d):Adding is successfully

Figure 20(c) and Figure 20(d) demostarted the simulation of a successful fingerprint registration by making use of **DOWN** push button.

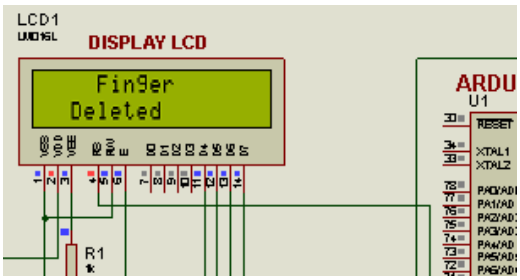

Fig. 20(e): Fingerprint Delected

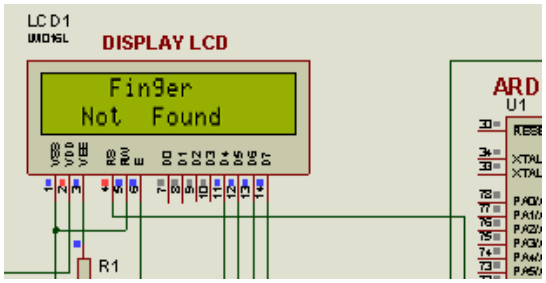

Fig. 20(f): Finger Not Found

Fig 20(e) and fig 20(f) demostrated deletiopn of template or if is not found by using DELETE push button and CANCEL.

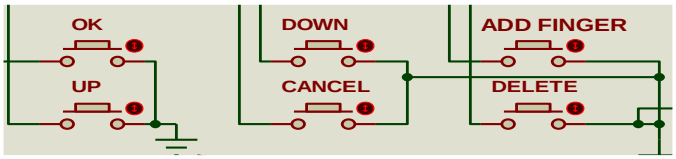

Fig. 21: Push Button

The above figure is the push button for registration and deleting of the template.

Matching Simulation

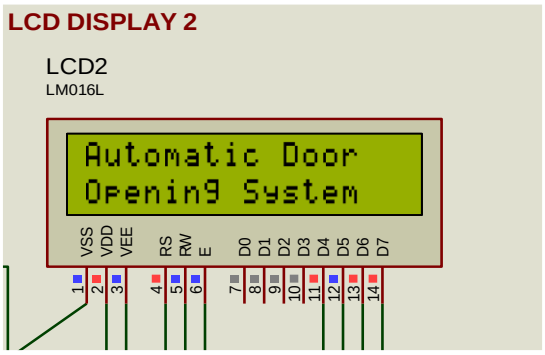

Fig. 21(a): Welcome Message

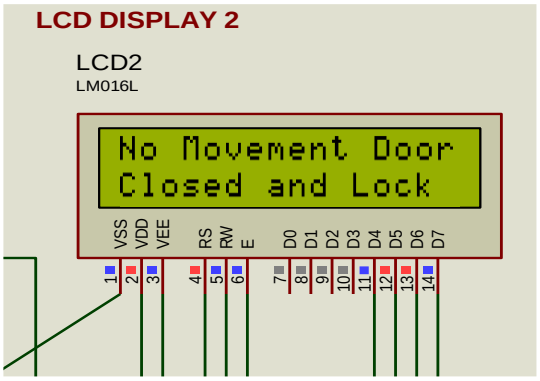

Fig. 21(b): State of the Sytem

Fig 21(a) Displayed the welcome message with 1munite delay and Fig 21(b) After 1minute of running the simulation the lcd will display NO MOVEMENT, DOOR CLOSED AND LOCK because no signal from sensor.

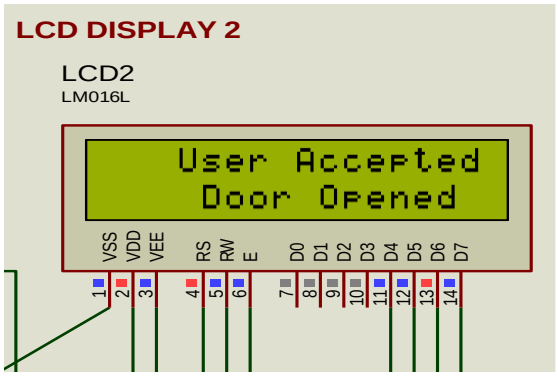

Fig. 21(c): Opening of the Door

The above figure 21 (c) demostrated when the matching button is push it compare the new template and if the user is

Abdulhakeem Ishola, Abdullahi Abubakar, Zayyanu Umar, and Musa Abubakar Alkali Tanko, Musa Ibrahim Kamba, "Automated Security Door System Using Fingerprint as Authentication for Access," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 9, pp. 118-129, 2023.

accepted, it activate the sensor for the motor to rotate for 1munite.

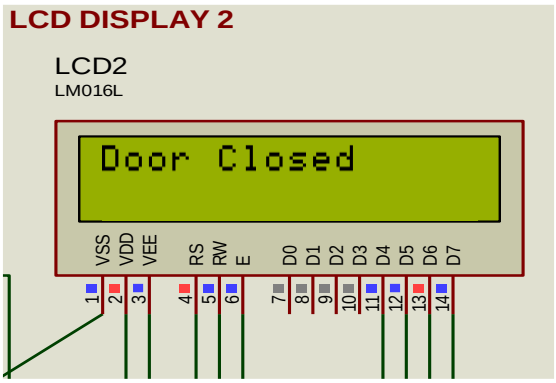

Fig. 21(d): Closing of the Door

The above figure 21 (d) demostrated closing of the door after 2 munites delay (Pause) and the motor stop and lock the door after rotating for another 1munite.

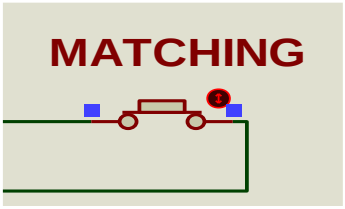

Fig. 22: Matching Push Button

The above figure 22 is the maching push button.

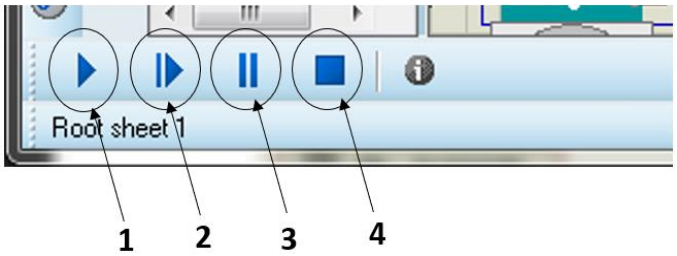

Fig. 23: Proteus 8 Professinal Function Button

1. Running/Playing the simulation.
2. Advance the simulation by one animation frame (running the simulation with pause).
3. Pause the simulation.
4. Terminating the simulation.

V. Discussion

A design to enhance the current system created by Saroj Singh (2020) was carried out in this study. In order to make the new system more user-friendly, we enhanced the source codes and proposed a method that offers an effective fingerprint matching template.

VI. Conclusion

In this study, a model of an automatic door that uses a security sensor (A fingerprint) was constructed, allowing for the door's electrical operation. It fixes the issues related to human security. It requires minimal to no human intervention to open and close the door, enhancing security and productivity. This system performs better in terms of time (Time Complexity) to recognize users when compared to other existing systems. Using an ATmega2560 board as the main board and an ATmega UNO board as a semi-board, which are both connected to one another using source code and connection wires in a schematic circuit, it was possible to model an automatic door that used a security sensor. MATLAB simulation software, which was precise and simple to grasp, was used to conduct and test the simulation.

VII. Recommendations

i. Putting this research into practice will be beneficial and a tremendous accomplishment, but it will also necessitate that the administrator supervise and protect all operations, including who gets access to the fingerprint data and who keeps the door maintained.

ii. Future study could include creating a database (storage software) for fingerprint registration in order to enroll a large number of people.

References

[1]. C. O. Akanbi1, I. K. Ogundoyin1, J. O. Akintola, K. Ameenah1 (2020) A Prototype Model of an IoT-based Door System using Double-access Fingerprint Technique. *Nigerian Journal Of Technological Development, VOL. 17, NO.2, JUNE 2020.*

[2]. C. D. Cortez, J. S. Badwal, J. R. Hipolito and J. C. Inalao, (2016) Development of microcontroller-based biometric locker system with short message service. *Lecture Notes on Software Engineering*, 4(2), 2016.

[3]. G. Jiang, X. Song, F. Zheng and A. M. Omer, Facial expression recognition using thermal, *Proc. 27th Annual Conference on IEEE Engineering in Medicine and Biology*, 2005.

[4]. HashemAlnabhi, Yahya Al-naamani, Mohammed Al-madhehagi, Mohammed Alhamzi (2020)

[5]. Hao Wang (2015) Design Of An Automatic Door System For An Automated Transit Network Vehicle. The Faculty of the Department of Mechanical Engineering San José State University.

[6]. HteikHtarLwin, AungSoeKhaing, and HlaMyoTun (2015) An Automated Door Control System using Biometric Technology. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. I (Jul - Aug 2017), PP 20-25 www.iosrjournals.org*

[7]. JiangshanGao, Yan Zhi (2019) Design of PLC Control System for Automatic Door. Open Access Library Journal, 6: e5891. https://doi.org/10.4236/oalib.1105891.

[8]. KHIN EI EI KHINE (2018) Simulation of Automatic Door Sliding Control System. International Journal of Scientific Engineering and Technology Research Volume.07, IssueNo.12, December-2018, Pages: 2000-2006.

[9]. HteikHtarLwin, AungSoeKhaing, HlaMyoTun (2015) Automatic Door Access System Using Face Recognition. International Journal Of Scientific & Technology Research VOLUME 4, ISSUE 06, JUNE 2015

[10]. Burak, Tolga, and Huseyin (2015) A low cost vein detection system using near infrared radiation, *Proc. IEEE Sensors Applications Symposium*, San Diego, California,.

[11]. Ganesh SahithiMurru, ChetanKakollu, Ashok Kumar Kenguva, P. Surya Chandra (2020)Biometric recognition: security and privacy concerns, IEEE Security and Privacy, 1(2), pp. 33-42.