Tropical Journal of Science and Technology, 2(1), 1-13, 2021
ISSN: 2714-383X (Print) 2714-3848 (Online) Available online at credencepressltd.com
DOI: 10.47524/tjst.21.3

Development and implementation of a password and fingerprint based circuit breaker

[1]Okhueleigbe, E.I. and [2]Okhaifoh, J.E.
Department of Electrical and Electronics,
Federal University of Petroleum Resources Effurun, Delta State, Nigeria[1,2]
Corresponding Email: [1]okhueleigbe.emmanuel@fupre.edu.ng
Cell: +2348038062904

Abstract

This study examined the problem faced during electrical accident investigation so as to allay fears, cloudy misgivings and suspicion of Re-energizing an already (or Purportedly) Isolated (De-Energized) Lines (Mechanically Padlocked) between the DISCO's linesman and operators in substation control room on one hand and factory maintenance technician and their control room operator on the other part during electrical accidents investigation, It tends to look at a solution that will be acceptable to all and sundry on the actual cause of the energization of an electrical line during repairs and maintenance which could have been due to a feedback current from another source but with this password and finger print circuit breaker, the linesman`s mind is at peace and his safety is maximally guaranteed.

Keywords: Electrical, password, accident, feedback, fingerprint

1.Introduction

1.1 Background of the study

Nowadays, electrical accidents and electrocution of linesmen and maintenance technicians are on the increase, while clearing faults in their network or carrying out maintenance on electrical installations especially those ones that require total isolation of the network electrical supply to carry out an effective repair; this accident is often due to ineffective communication between the electrical control room and maintenance staff. This research gives a solution to this problem to ensure optimal safety of linesmen and the maintenance team.

Electrical Accidents is defined as an undesired effect caused by electric current resulting to injury /death to person or damage to property (ELSAKERHETSVERKET –National Electrical Safety Board, Sweden); Furthermore; Samuel Pamah in his book – ELECRICAL ACCIDENTS PREVENTION 2003 stated that " Statistics of causes of preventable electrical accidents recorded in the past three years shows that 60 percent were of common causes while 30 percent occurred due to other defects, similarly, the alarming increase of these accidents cases reported rose by 20 percent between 2010-2014, Samuel Pamah (2003), Haruna H.N. et al (2018).

It is worthwhile to note that statistics from Nigerian Electricity Management Services Agency (NEMSA) Vol III, 2018 – The body statutorily empowered to investigate all electrical accidents and electrocution shows that 1 out 3 electrical accidents are 2nd party i.e staff or persons empowered by the Generating company (GENCO's), the Transmission Company of Nigeria (TCN) and the Distribution Company (DISCO's) NEMSA Newsletter – 3rd Quarter Edition (October 2018), which was corroborated by

Nigerian Electricity Regulatory Commission (NERC) (NERC 2nd Quarterly Reports Page 5, July 2018); The data above, coupled with my interaction during Electrical Accidents investigations and factory inspection about misgivings and suspicion between the DISCO's linesmen and operators in substation control room on one part and factory maintenance technician and their control room operator on the other part spur me to embark on the solution this problem. It is imperative to point out that majority of distribution and transmission substation in Nigeria are built over 30 years ago by the defunct Nigeria Electric Power Authority (NEPA) which are now aged, obsolete and not in tandem with latest technology which makes it to be manually padlocked. In this research the control (ON/OFF) of the electrical lines lies with linesman or the maintenance technician as the case may be. This research is purposely designed in such a way that maintenance staff or linesmen have to enter the password to ON/OFF the electrical line, if there is any fault in electrical lines or network, the linesman will switch off the power supply to the line by entering an assigned or dedicated password which will automatically deactivate the circuit breakers and comfortably carry out repair on the electrical line, and after coming back to the substation, the linesman switch on the supply of the deactivated line by entering same password again. Separate passwords are assigned for each electrical linesman and once a particular password is 10 entered it. There will also be an overriding password to curtail the excesses of the password holder during unwholesome act; this simulation will only be at the disposal of senior management personnel of the organization. The system can also be extended to feeder pillar access as presently all manners of unautho rized personnel have access to the feeder p illar in substations despite the fencing and mechanical lock & key (Gupta, 2015; Cappellir, 2003; Cappelli et, al., 2016; Sukthanker, 2019).

2.Methodology

Research methodologies deployed make use of a systematically programming approach of a well-defined procedure that should be followed in caring out a thorough research work. An adequately suitable methodology would ensure a very detail research work and ensure a higher degree of accuracy and efficiency is adopted. In other to attain quiet a reasonable acceptance of the research work, the internationally accepted software engineering model was used, which is During authentication, the biometrics of the user is captured again and the extracted features are compared (using a matching algorithm) with the ones already existing in the database to determine a match. It ha s been established that physical achieves a re not always helpful a much better alternative is to use biometrics concept that can facilitate stronger security to the problem of exam impersonation (Valvano, 2011; Tang Homan and Sunny, 2011; Valetin et, al., 2014; KarlJ & Wittenmark, 2002). This implies the creation of database management system (DBMS) which ensure that computer records are kept up to date and made available on demand to those who need them for planning and operational purpose (Simon Cole, 2011; Anil et, al., 2012; Mazidi, 2012).

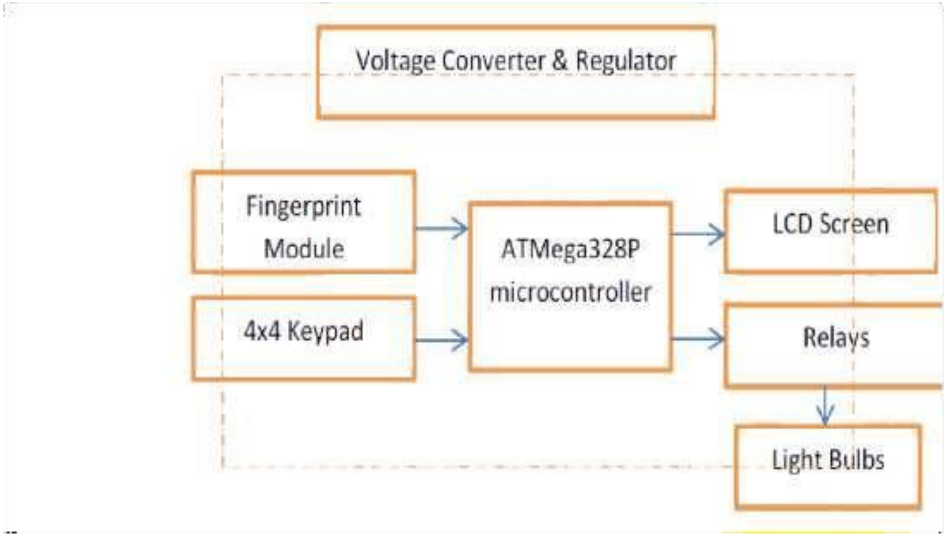


Fig.1: Block diagram of a finger print and password circuit based breaker

3. Implementation

3.1 Concept

In identification, the system recognizes an individual by comparing his/her biometrics with every record in the database. In general, biometric identification consists of two stages: Enrolment and Authentication. During enrolment, the biometrics of the user is captured (using a fingerprint reader, which are likely to be an optical, solid state or an ultrasound sensor or other suitable device) and the unique features are extracted and stored in a database as a template along with the user identification. The objective of the enrolment module is to admit a user using his/her identification and fingerprints into a database after feature extraction. These features form a template that is used to determine the identity of the user, formulating the process of authentication. The enrolment process is carried out by the Device Administrator.

3.2 Operation

In a normal control room, the source of power supply is to use a UPS (Uninterruptible Power Supply) so as to back up the system, in case of power failure. The system need regulated DC power supply to power the components and the power need to be regulated, these components need stable power supply and at the certain limit. At Start-up, a welcome message is displayed on the LCD display: (“Fingerprint Authentication”) the name of the system, then two seconds later it will display for the user to place the finger on the fingerprint scanner for the fingerprint scan to be captured for authentication. The comparison is done by the microcontroller, comparing the recently captured with the one in the database stored after registration phase, if there is a match then the system will ask for a passcode and if the passkey is correct then the microcontroller de-activate the Line relay for maintenance work. If there is no match between the fingerprints then the system will display that access denied, user not registered, it will never ask for passkey. To sum the operation up, this system consists of a fingerprint scanner connected to a microcontroller circuit. The person needs to first scan his/her finger on the scanner. The microcontroller then checks the person’s fingerprint validity.

3.3 Stages involved

The design of the research is done in two stages, the hardware part and software section. The software part is achieved using Proteus Lab Centre 8.0 software and microcontroller.

Programming done using Embedded "C" language. The hardware (device) comprises of the microcontroller, the fingerprint scanner, Motor Driver (L293D), DC motor, small door, LEDs, Capacitors, Resistors and Diodes.

3.4 Fingerprint sensor

Fingerprint sensor modules made fingerprint recognition more accessible and easier to add to our design. These modules come with storage device or FLASH memory to store the fingerprints and work with any microcontroller or system with Transistor-Transistor Logic TTL serial. These modules can be added to security systems, door locks, time attendance systems, and much more.

Specifications

- ✦ Voltage supply: DC 3.6 to 6.0V
- ✦ Current supply: <120mA
- ✦ Backlight colour: green
- ✦ Interface: UART
- ✦ Bad rate: 9600
- ✦ Safety level: five (from low to high: 1,2,3,4,5)
- ✦ False Accept Rate (FAR): <0.001% (security level 3)
- ✦ False Reject Rate (FRR): <1.0% (security level 3)
- ✦ Able to store 127 different fingerprints

The sensor has six pins that are labelled in figure 2.

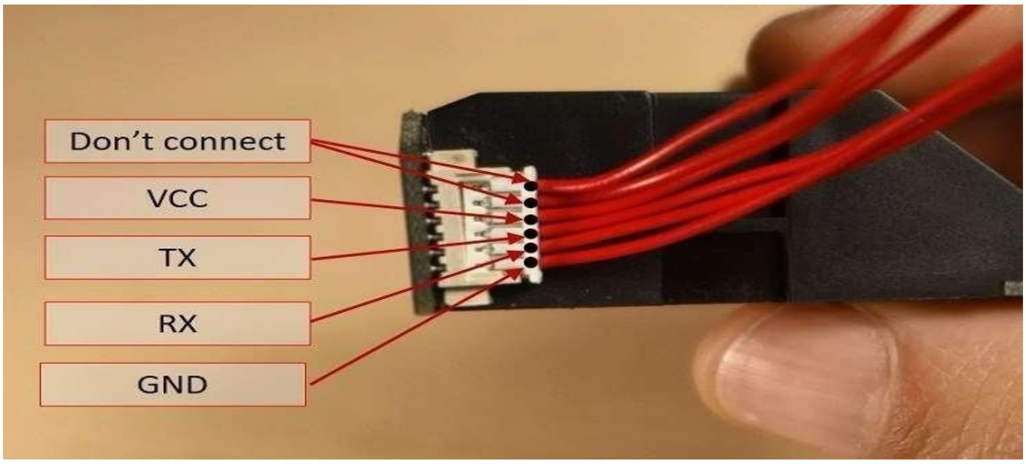


Fig. 2: Fingerprint sensor pin-out

The fingerprint sensor module used in this research came with really thin wires, so soldering breadboard-friendly wires was used. With different colours according to the pin function, In this case:

- ✦ DNC – white wires
- ✦ VCC – red wire
- ✦ TX – blue wire
- ✦ RX – green wire
- ✦ GND – black wire

Table 1: How to wire the sensor.

Fingerprint Sensor	Microcontroller pins
VCC	5V (it also works with 3.3V)
TX	RX (digital pin 2, software serial)
RX	TX (digital pin 3, software serial)
GND	GND

3.5 Matrix keypad

Keypad is an input device, sometimes part of a standard computer keyboard, consisting of a separate grid of numerical and function keys arranged for efficient data entry according to (American Heritage Dictionary, 2014). Keypads are often used as a primary input device for embedded microcontrollers. The keypads actually consist of a number of switches, connected in a row/column arrangement as shown in Figure 3

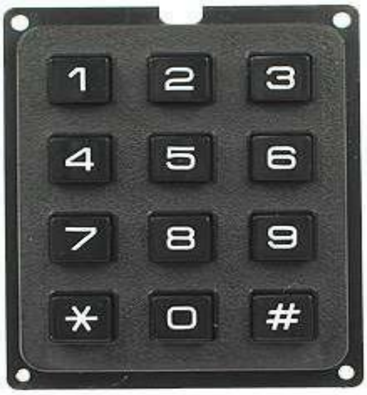


Fig.3: A numeric keypad

3.6 Atmega 328p microcontroller

The ATmega328 is a single chip microcontroller created by Atmel in the MegaAVR family. The Atmel 8-bit AVR RISC (Reduced Instruction Set Computer) based microcontroller which combines 32KiloByte-ISP flash memory with Read &Write capabilities, 1 kB EEPROM, 2 kB SRAM, 23 General Purpose I/O lines, 32 general purpose working registers, 3 flexible timer/counters with compare modes, Internal and External Interrupts, Serial Programmable USART, a byte-oriented 2-Wire Serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP & QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts.

The device achieves throughout approaching 1 MIPS per MHz. (Source: *ATMEL ATmega328 datasheet*)

Fig..4: ATMega328P microcontroller

ATmega328 is commonly used in autonomous systems where simple, low-powered, low-cost microcontroller is needed. Perhaps the most common implementation of this chip is on the popular Arduino development platform, namely the Arduino models.

Table 2: AT mega 32P microcontroller parameters and their function

Parameter	Value
CPU type	8-bit AVR
Performance	20 MIPS at 20 MHz
Flash memory	32 kB
SRAM	2 kB
EEPROM	1 kB
Pin count	28-pin PDIP, MLF, 32-pin TQFP
Maximum operating frequency	20 MHz
Number of touch channels	16
Hardware QTouch Acquisition	No
Maximum I/O pins	23
External interrupts	2
USB Interface	No
USB Speed	–

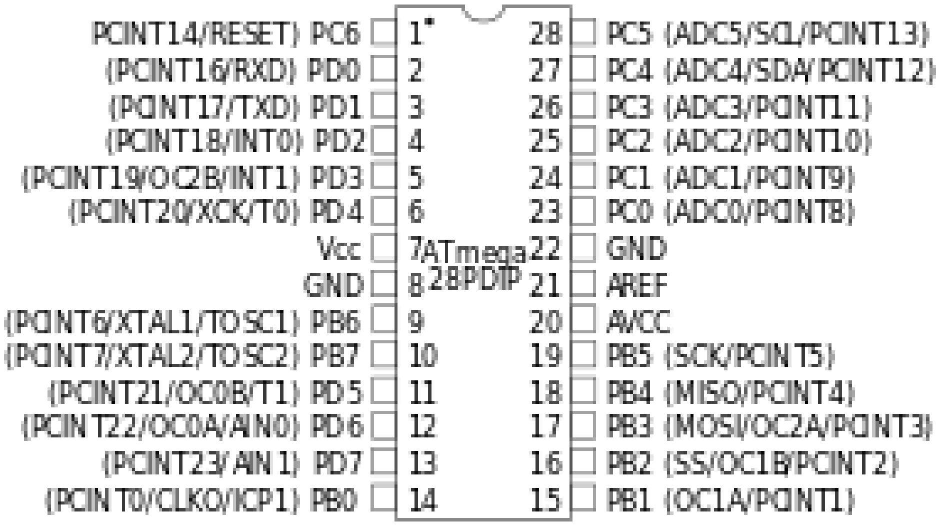


Figure. 5: Pin description of ATMega328P microcontroller

3.7 Electromagnetic relay

A relay is a device, usually consisting of an electromagnet and an armature, by which a change of current or voltage in one circuit is used to make or break a connection in another circuit or to affect the operation of other devices in the same or another circuit.

There many types of relay; these include latch relay, reed relay and solid state relay. A relay will switch one or more poles each of whose contact can be thrown by energizing the coil in one of two ways. When an electric current is passed through the coil it generates a magnetic field that activates the armature and the consequent movement of the movable contact either makes or breaks (depending upon construction) a connection with a fixed contact. If the set of contacts was closed when the relay was de-energized, the movement opens the contacts and breaks the connection, and vice versa if the contacts were open. When the current to the coil is switched off, the armature is returned by a force, approximately half as strong as the magnetic force, to its relaxed position.

Usually this force is provided by a spring, but gravity is also used commonly in industrial motor starters. Most relays are manufactured to operate quickly. In a low voltage application this reduces noise; in a high voltage or current application it reduces arcing.

When the coil is energized with direct current, a diode is often placed across the coil to dissipate the energy from the collapsing magnetic field at deactivation, which would otherwise generate a voltage spike dangerous to semiconductor circuit components. Some automotive relays include a diode inside the relay case. Alternatively, a contact protection network consisting of a capacitor and resistor in series (snubber circuit) may absorb the surge. If the coil is designed to be energized with alternating current (AC), a small copper "shading ring" can be crimped to the end of the solenoid, creating a small out-of-phase current which increases the minimum pull on the armature during the AC cycle.

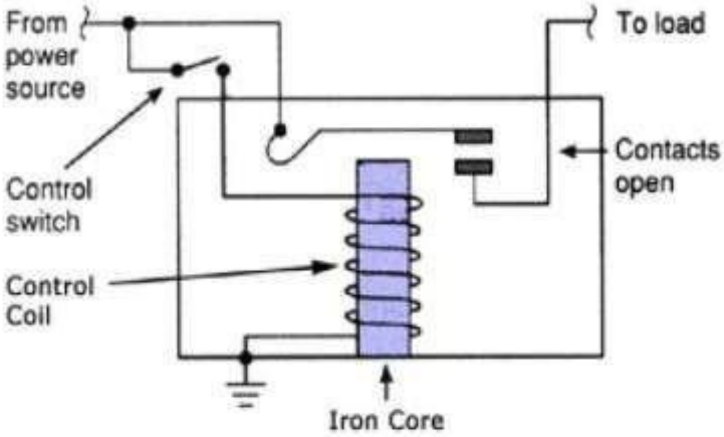


Figure 6: An electromagnetic relay

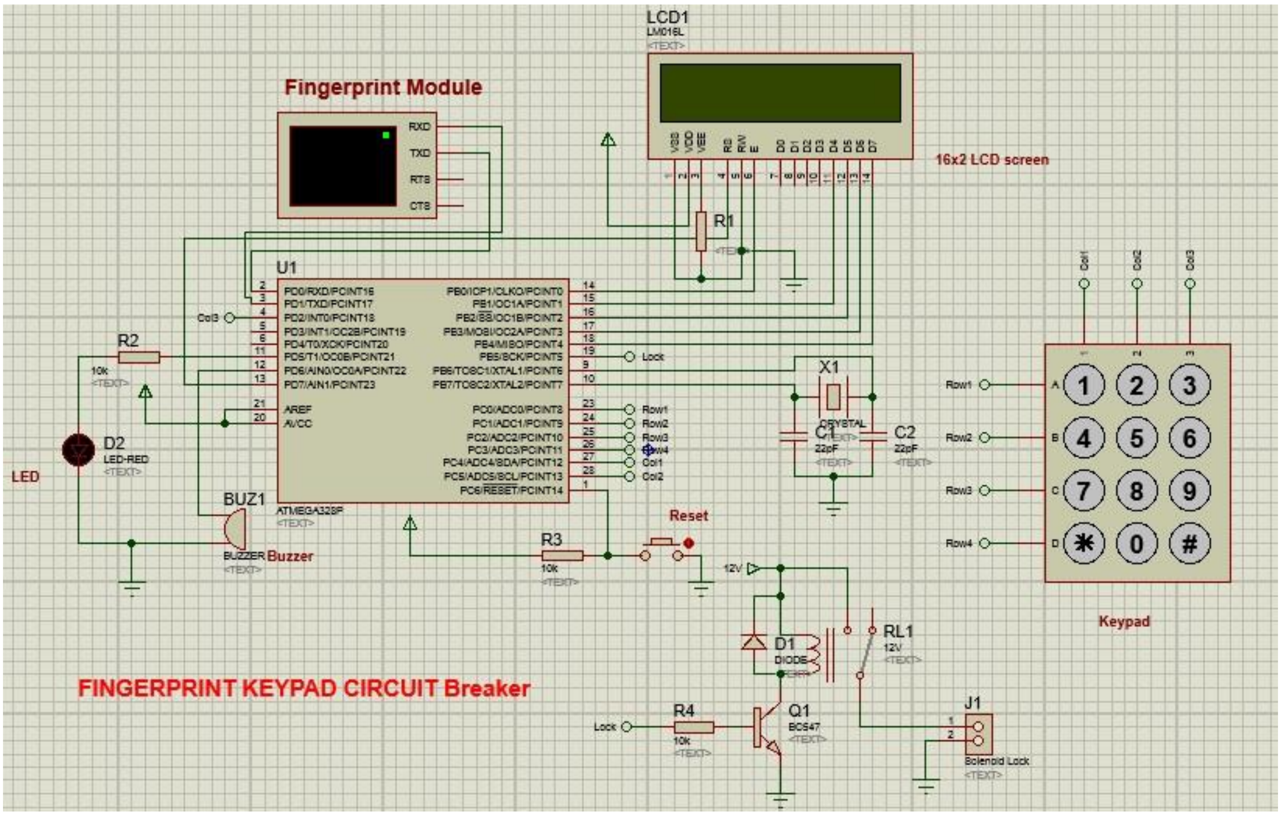


Fig. 7: Complete schematics diagram

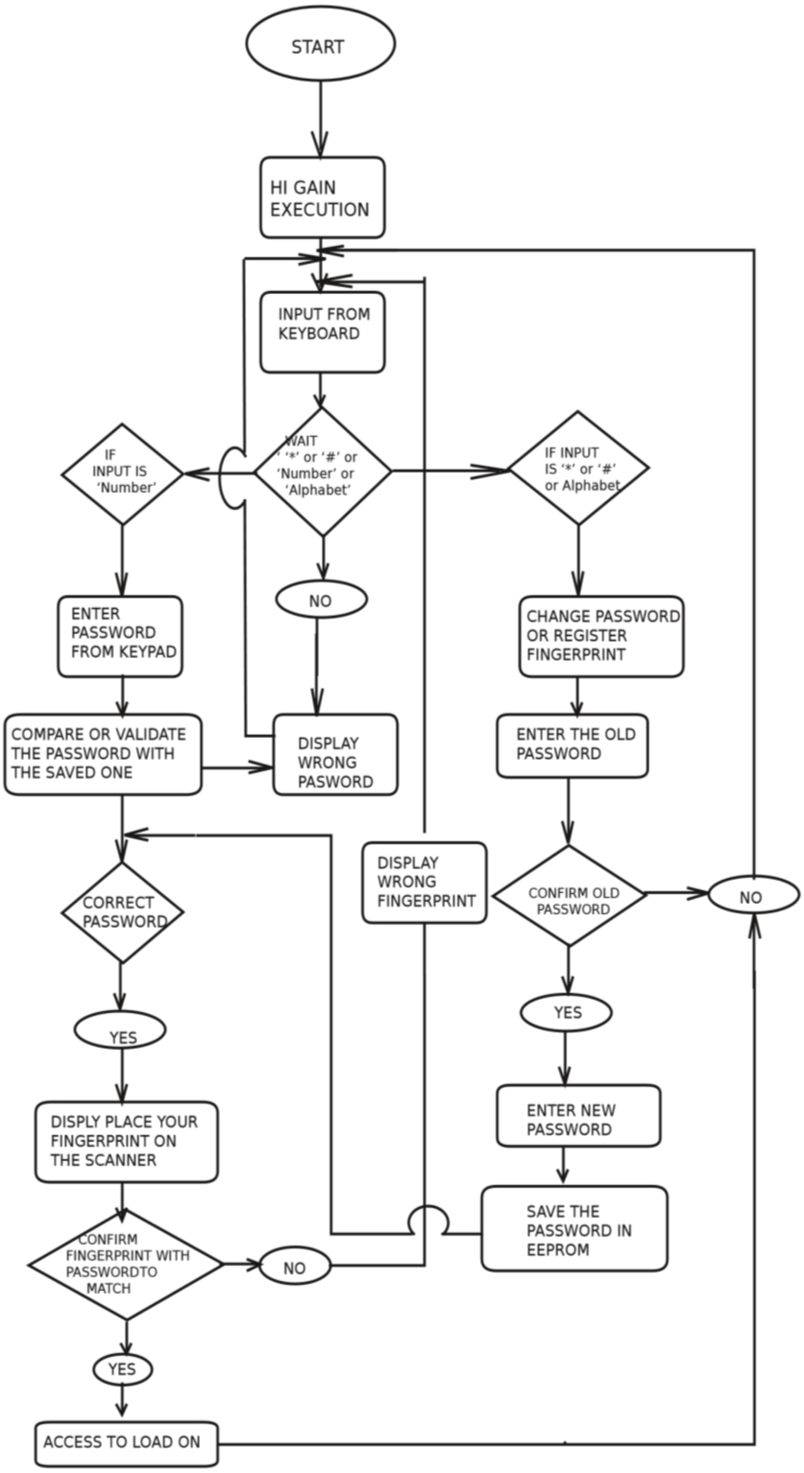

START
HI GAIN EXECUTION
INPUT FROM KEYBOARD
IF INPUT IS 'Number'
WAIT '*' or '#' or 'Number' or 'Alphabet'
IF INPUT IS '*' or '#' or Alphabet
NO
ENTER PASSWORD FROM KEYPAD
CHANGE PASSWORD OR REGISTER FINGERPRINT
COMPARE OR VALIDATE THE PASSWORD WITH THE SAVED ONE
DISPLAY WRONG PASWORD
ENTER THE OLD PASSWORD
DISPLAY WRONG FINGERPRINT
CORRECT PASSWORD
CONFIRM OLD PASSWORD
NO
YES
YES
DISPLY PLACE YOUR FINGERPRINT ON THE SCANNER
ENTER NEW PASSWORD
SAVE THE PASSWORD IN EEPROM
CONFIRM FINGERPRINT WITH PASSWORDTO MATCH
NO
YES
ACCESS TO LOAD ON

Fig. 8: Flow chart of password and fingerprint based circuit breaker

3.8 Implementation

The implementation of this research was done on the breadboard. The power supply was first derived from a bench power supply in the electronics laboratory. To confirm the workability of the circuits before the power supply stage was soldered. The implementation of the project on bread board was successful and it met the desired design aims with each stage performing as designed.

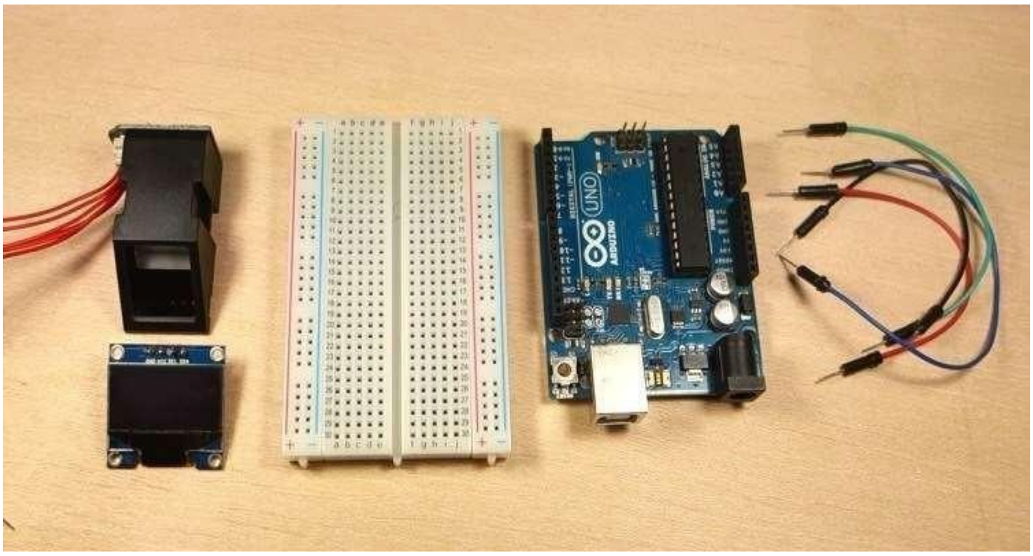


Fig. 9: Project bread boarding

3.9 Simulation

The whole electrical part of the project was simulated on PROTEUS simulation platform before the soldering work commenced to observe the operation of the whole research.

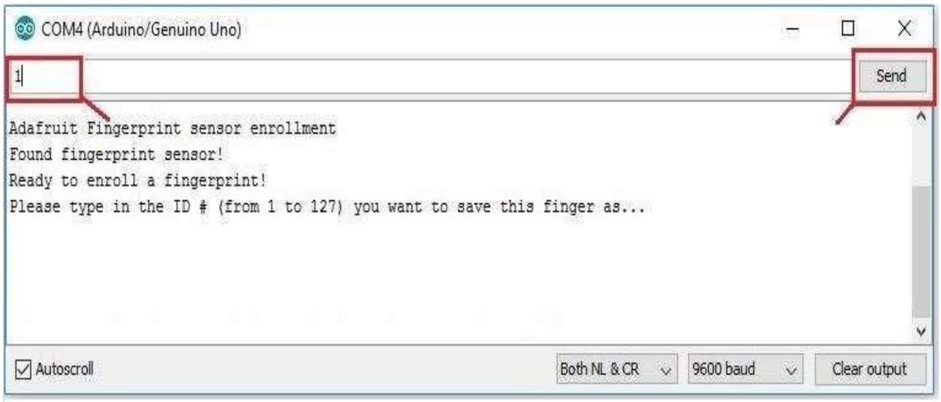
3.9.1 Soldering

The various circuits and stages of this research were soldered in tandem to meet desired workability of the research. The power supply stage was first soldered before the microcontroller, digital (LCD) display and finger print reader module stages were done. The soldering of the project was done on Vero- board, and was soldered on two small sized Vero boards. The first Vero board contains the power supply stage, the microcontroller stage with the finger print reader module interface stage; the second Vero board has the transistor switching for driving the motor used to automate the door.

3.9.2 Testing

1.**Enroll a new fingerprint**

Having the fingerprint sensor module wired to the microcontroller, new fingerprint can be enrolled by following a sample program from **Adafruit Fingerprint Library installed to the Arduino Development Environment.** Code is uploaded while operations can be seen on the serial monitor at a baud rate of 9600. **A unique** ID should be enter to the serial monitor be for the fingerprint to be captured



```
Adafruit Fingerprint sensor enrollment
Found fingerprint sensor!
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Fig. 10: Fingerprint enrolment

Place your finger on the scanner and follow the instructions on the serial monitor.

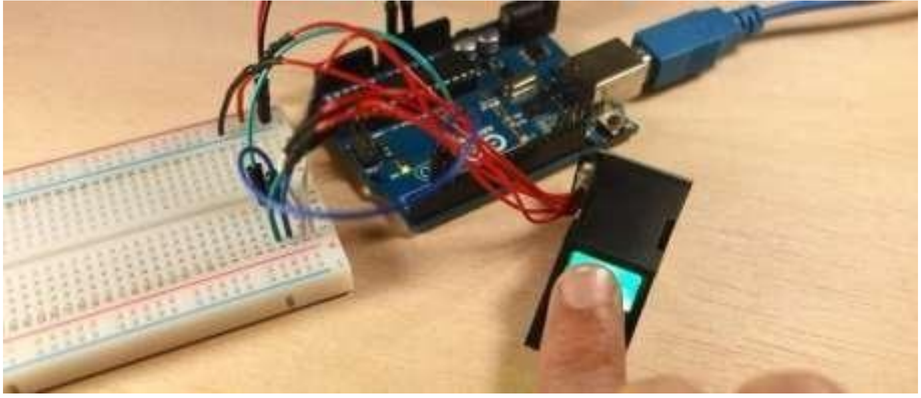


Fig. 11 Finger enrolment with finger on scanner

If finger is correctly places, the serial monitor will display “**Prints matched!**” message, as shown below, test fingerprint is successfully stored. If not, repeat the process until you succeed. Store as many fingerprints you want using this method.

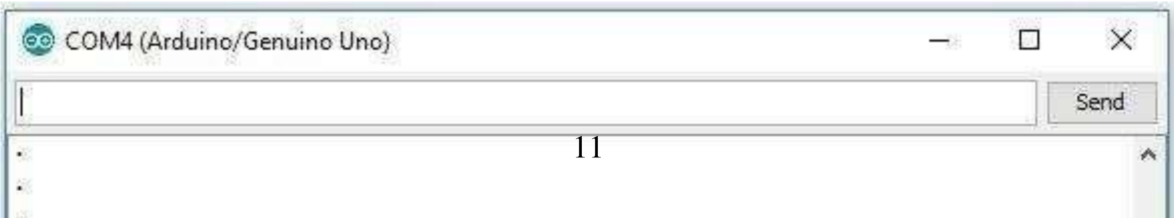


Fig.11: Successful finger enrolment

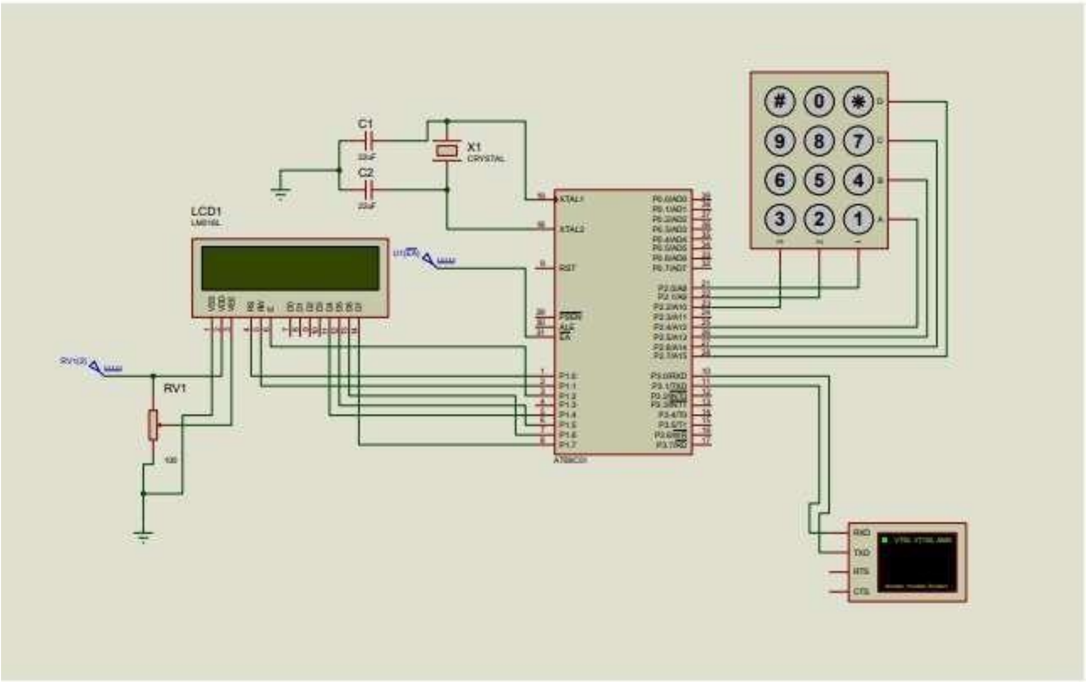


Fig. 12: Simulations of the entire project

Conclusion

The design is achieved by interfacing a UART (Universal Asynchronous Receiver – Transmitter) Fingerprint reader with the ATMega328P Microcontroller, it is the brain box that controls the whole Circuit breaker System. LCD (Liquid Crystal Display) status display is employed to show the operating status of the system. Relay activates and de-activates the Line once user has been authenticated which is known by the glowing of a bulb. Finger print input stage was implemented using the UART port to communicate with the microcontroller. The development guarantees security for illegal intrusion on the Line during maintenance work.

References

Anil. K., Jain, A. R. & Prabhakar. S., (2012). Fingerprint Matching using Minutiae and Texture features", proc. International Conference on Image Processing (ICIP), pp 282-285, Greece, October 7-10, 2012.

Cappelli R., Ferrara, M., & Maltoni D., (2016). The Quality of Fingerprint Scanners and Its Impact on the Accuracy of Fingerprint Recognition Algorithms. In *Processing of Multimedia Content Representation, Classification and Security* (MRCS2006), pp 10-16.

Cappellir, (2003). *Handbook of Fingerprint Recognition.* Chapter synthetic fingerprint generation. Springer, New York.

Gupta, B.R., (2015). Power System Analysis and Design.

Haruna H.N. et al 2018. Review of Electrical Accidents and Electrocution in NESI NEMSA Newsletter – 3rd Quarter Edition

Jonathan W. Valvano, (2011). Embedded Microcomputer Systems: Real Time Interfacing.

Karl J. Astrom, & Bjorn Wittenmark, (2002). Computer Controlled Systems: Theory and Design. pp 23-34

Mazidi, J. G., (2012). The 8051 Microcontroller and Embedded systems Pearson Education. 2012.

Nigerian Electricity Regulatory Commission (NERC) {NERC 2nd Quarterly Reports Page 5, July 2018.

Samuel P. (2003). *Elecrical Accidents Prevention* New Age Publisher.

Simon C., (2011). Suspect Identities: A history of fingerprinting and criminal identification (Cambridge, Mass.: Harvard University Press, 2011), pp 60-61.

Sukthanker, G., (2019). Face Recognition: A critical look at Biologically-Inspired Approaches *2:* 45-48.

Tang H. & Sunny E., (2011). Face Recognition Review. Term paper, Department Computer Science and Engineering, Chinese University of Hong Kong, Shatin.

Valetin D, Abdi H, O' Toole A.J. & Cottrell G.W., (2014). Connectionist models of Face Processing: A survey. Pattern Recognition *27*(9):1209-1230.