Research Article / Review Article

FUPRE JOURNAL 10(2):01-17(2026)
https://doi.org//10.60787/FJSIR.v10i2.01-17

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Android Based Lock System Using Bluetooth

AVWORO, O. L.

Department of Electrical Engineering, Federal University of Petroleum Resources, Effurun, Delta State, Nigeria

ARTICLE INFO

Received: 23/05/2006
Accepted: 23/08/2026

Keywords

Android, Bluetooth, Home automation, Internet of things, Microcontrollers, Password authentication, Smart lock system, Wireless security

ABSTRACT

Lock systems are very popular devices in our everyday life for safety purposes but due to the constant loss and theft of keys, a lot of automated lock systems have been built to combat these issues but they all have serious short comings mostly with the price point and complexity of the circuitry. The necessity of a low-cost electronic security system designed in co-ordination with other security measures is always there in our society to reduce the risk of intrusion. Keeping this problem in mind, this project titled Android based lock system is mainly aimed at solving the issues associated with the available automated lock systems. The lock system consists of an Electro-magnetic lock, an android-based mobile phone graphical user interface (GUI) designed for easy use, a Bluetooth module interfaced with a micro controller and an LCD display. This research is divided into three parts, which is the mobile application graphical user interface (GUI), which makes it possible to input the password and it's based on Android, the Bluetooth receiver circuit based on a micro controller and the LCD screen that displays the status of the lock system. The system operation is simple. The android phone is connected via Bluetooth to the microcontroller, the user is asked on the mobile phone to input password to unlock the lock system and when the password is keyed in the data is transmitted to the Bluetooth receiver and if it corrects the LCD display shows access granted and unlocks the system.

1. INTRODUCTION

Advancement of technology things are becoming simpler and easier for us. Automation is the use of control systems and information technologies to reduce the need for human work in the production of goods and services. In the scope of industrialization, automation is a step beyond mechanization. Whereas mechanization provided human operators with machinery to assist them with the muscular requirements of work, automation greatly decreases the need for human sensory and mental requirements as well (Sriskanthan *et al.* 2002). Automation plays an increasingly important role in the world economy and in daily experience. Automatic systems are being preferred over manual system. Through this project we will try to show automatic control of a lock as a result of which security is improved to some extent. In this digital age, every device and operation has become digital based. Now with electronic based lock systems, it is easier to control locks. The android-based lock system does not need a key to unlock or lock. The electronic system is controlled by an android smart phone in which the

*Corresponding author, leslieavworo@gmail.com
https://doi.org//10.60787/FJSIR.v10i2.01-17
©Scientific Information, Documentation and Publishing Office at FUPRE Journal

application is installed (Rathnayaka *et al.* 2011). The keyless lock is an electronic circuit-based device. The working mechanism of this locking system is very simple. It works using Bluetooth technology; the phone's Bluetooth connects with the Bluetooth of the lock system. The authenticated person has to enter the unique code using the android phone.

You can install a keyless lock system in your house as well as in buildings and offices. With this system, you will never be in tension of leaving sensitive areas out of your supervision. Lastly, it is inexpensive to build compared to other available lock system (Felix and Raglend 2011).

With the increase in theft rate and automated property protection, different automated lock systems have been introduced in other to enhance security in homes, offices and industries (Al-Shammaa and Al-Majidi 2013). As with most electronics, there are problems to these systems such as the cost of implementation and complexity in the architecture, with some systems having no user interface, which does not serve the purpose of a user-friendly automation system (Mahajan and Khadse 2020).

This project is another way of developing an automated lock system but in this case, it has a friendly user interface (GUI). This project uses Bluetooth technology for communication, which is already available in most mobile phones in our present day making this automated lock system more cost effective (Arredondo B. 2013).

Though there have been many other forms of automated lock system but those systems are prone to hacking and inconsistencies. Good examples are the fingerprint, iris scanner and keypad input lock systems (PIC Microcontroller 2017). The finger-print system faces a lot of inconsistencies due to the fact that it only works 80% of the time because little moisture on the print can lead to an error in reading the print (Quispe and Mamani 2023). In the case of the iris scanner lock system, they fail when one wears contact lenses or cannot open their eyes for a long period of time while in front of intense luminosity and for the keypad system, due the fact that the keypad is always presented to everyone, an unauthorized person can easily hack it by simply trying different ranges of passcode till they finally get the right code making the system easy to hack but it the case of this project, all those disadvantages have been corrected to avoid bridge of security (Theint *et al.* 2026).

Voice recognition can easily be imitated, facial recognition suffers from illumination and change of faces due to age and lastly signature recognition security lock has suffered from the fact that there are illiterate people that are incapable of signing and signature patterns are easily copied (Sanchez and Martin 2024).

To overcome these problems, this project is based on developing an android-based lock system. This project will apply the use of a personal android smartphone, which contains the proprietary security lock application to open locks (Almheiri and Alblooshi 2023). This is a more secure system since the phone, the application and the passcode is personalized to the user only (Pannirselvam and Zohari 2025).

2 METHODOLOGY AND MATERIALS

2.1 System Design

The project basically consists of two main parts the hardware and the software, which are interconnected together in order

to get a completely functional system. This chapter shows the method use to implement the project. The chapter shows system technical design in the block diagram form, methodology and flow charts used in the project.

2.1.1 System Description

It is important to know how the overall project is working before the detail project design. The system is described by the block diagram in the Figure 3 below, it requires a 240V main source. The source is converted into 12V DC by an adaptor which is then connected to the lock system. At the transmitter side, the only design is the Android software remote control system. Typical design of the Android software to control the lock system can be seen in Figure 1.



Figure 1: Gui Window for The Android Software to Control the Relay Gate.

From the proposed GUI window, on the left shows the "KEY IN PASSWORD" and on the right shows the "SEND". By keying in the right password and clicking on "SEND", the lock should open. Similarly, if the password is incorrect, by clicking on "SEND" button, the lock stays close. Also, there is a small notification in the Android GUI window used to indicate the ready function. This is important to tell user about the successful pairing of the Bluetooth signals (Abbas *et al.* 2025).

2.2 Block Diagram

Figure 3.3 below shows the system block diagram design for the Bluetooth control system. As seen in the diagram, the main component is the PIC16F877A microcontroller. This microcontroller is power up by 5V DC power supply and receives a clock pulse from the 4MHz crystal oscillator also connected to the PIC controller is a LCD which displays the status of the lock.

The microcontroller receives signal from the Bluetooth module connected to it and powered by a 3.3V DC. The Bluetooth on the mobile is connected to the Bluetooth module on the control system wirelessly to control the lock.

The entire circuit operation basically depends on the program design or the program embedded inside the microcontroller. The programing design will be shown at the software design section.

Figure 2 shows a functional block diagram that schematically represents the regulated power supply.

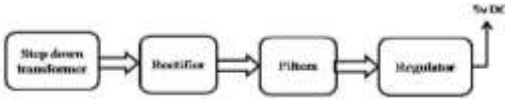


Figure 2: Power Supply Block Diagram

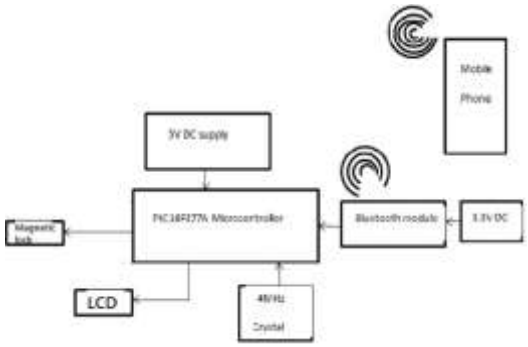


Figure 3: The System Block Diagram.

2.3 Hardware Design details

This section presents the circuit design and the software design for the system control to open and to close the relay gates.

Circuit

Based on the block diagram shown in the Figure 3, the complete circuit diagram shown in Figure 4 shows the complete circuit diagram for the Bluetooth receiver

to control the relay gate.

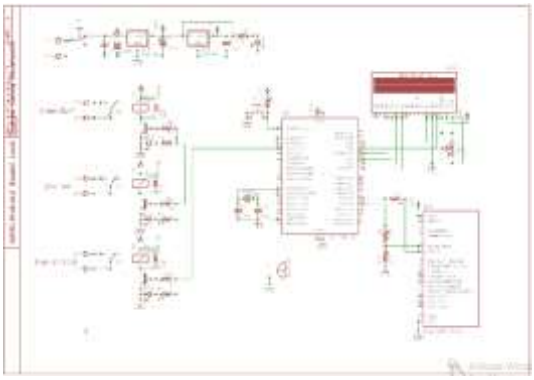


Figure 4: Bluetooth Remote Control Circuit Diagram

As seen in Figure 4, most of the components and their function will be later explained in chapter 4.

The transistor 2N2222A is a high current transistor. It has a gain of 40. Therefore, if the output of the microcontroller is digital HIGH, the current produce at the base of the transistor is:

=4.3mA (1)

The collector of the transistor used to trigger the relay is:

$$IC = 40 \times 4.3mA \quad (2)$$

=0.172A (3)

For the LED, each taking the current:

=5.95mA to light up. (4)

2.4 Software design or flow chart

The software design flow chart consists of two parts: embedded C program design for the microcontroller to detect the Bluetooth signal and trigger the relay gate to open or close. Lastly, is the android application program designed for the remote control of the lock system.

The discussion will begin from the embedded C program design for the microcontroller and next will be the android program.

2.4.1 Flowchart for microcontroller to trigger the relay to on or off the magnetic lock

This section will show the flow chart of the program design for the microcontroller to control the relay to on or off the magnetic lock. The detail of the coding will be shown in later on. The Figure 5 shows the flow chart for the Bluetooth signal detection and relay circuit triggering.

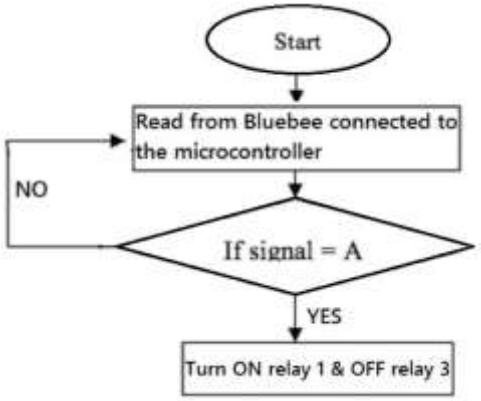


Figure 5: Flowchart Of Program Design to Detect Bluetooth Signal and Trigger the Relays

The program design for the microcontroller consists of infinite loop function, “if” function, “read” function and “trigger output high” function.

The program will constantly try to detect input signal from the Bluebee Bluetooth chip. Lets assume A is the correct password and B is a wrong password. If the Bluebee Bluetooth chip receives character "A" from the smart phone, the microcontroller will trigger the magnetic lock relay to turn off which unlocks the lock otherwise if character "B" is detected the state of the relay stays the same which keeps the magnetic lock locked. The system is made up of three relays namely relay1, relay2 and relay3. The relay1 is a green notification light indicating access

granted, relay2 is a red notification light indicating wrong password input while the relay3 is connected to the magnetic lock therefore its always on making the system lock.

2.4.2 Android program design

The Figure 6 show the Android remote control platform flowchart.

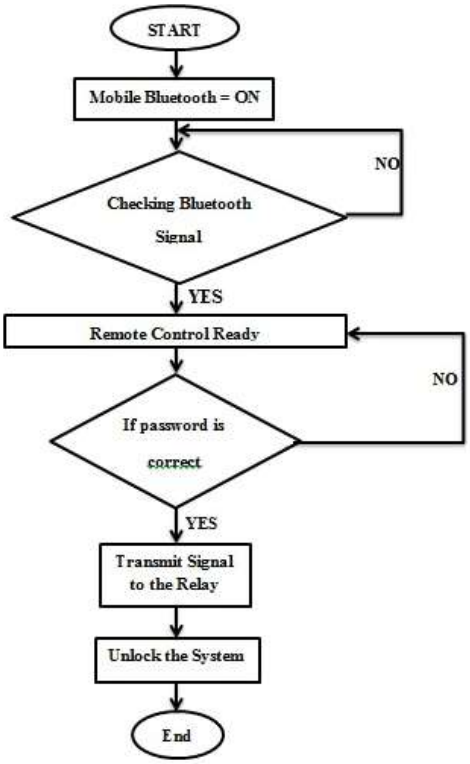


Figure 6: Android Remote Control Platform Programming

The android remote control platform is a simple platform. It has a programming function using "if" command. The "if" command is used to check the condition of the keyed in password. When the keyed in password is correct a signal is sent out to turn off the relay, which opens the magnetic lock. When the keyed in password is incorrect a signal is sent to the relay to keep is present ON state. In a case where the header P is not typed before the password or the keyed in password is not up to seven digits the program will not work or response from them. The keyed in password from the Android mobile phone in sent to the Bluetooth module in the form of hexadecimal which is then transmitted to the microcontroller where it is broken down into binary.

2.5 Hardware and Software Implentation

The components and software tools showcased here. The complete prototype outlooks also presented in this implementation section.

2.5.1 Components used in the project

This section presents the important components used in the project. The section will show the pictures of the components and explain their functions or purposes to use it in the project.

2.5.2 Bluetooth Chip (Blue-Bee)



Figure 7: Bluebee Chip

Table 1: Technical Data for the Bluebee Chip

Parameters	Technical Information
Input voltage	3.3V
Input current	5mA
Frequency	2.4GHz
Moderation	ASK
Transmission or detection range	100m
Data rate	9600kbps

Figure 7 shows the Bluetooth chip and

table 1 shows technical data about the chip. This Bluetooth chip is selected in the project because it is easy to use and control through a simple command. Apart from that, the chip can receive the Bluetooth signals from the transmitter and also acts as a transmitter to transmit the Bluetooth signals. The cost for this chip is around RM 200. The pins configurations for the chip can be seen in appendix.

3.5.3 PIC16F877A Microcontroller

The Figure 8 and the table 2 shows the microcontroller used for this project and its characteristics.



Figure 8: Pic16f877a Microcontroller

Table 2: Technical Data for Pic16f877a Microcontroller

Parameters	**Technical Information**
Input voltage	5V
Input current	50mA
Frequency	0 - 20MHz
Memory	318kB
No. of ports	5
Programming	Assembly or embedded C program

The microcontroller is a key component in the project. It is used to read the Bluetooth signals, identify the signals and turn the relay gate open and closed accordingly.

2.5.4 LM7805 Voltage Regulator

The Figure 9 and the table 3 shows the LM7805 voltage regulator and its technical information.

Figure 9: Lm7805 5v Voltage Regulator

Table 3: Technical Information About the Lm7805

Parameters	**Technical Information**
Input voltage	6V to 20V
Output voltage	5V
Output current	1A
No of pins	3

LM7805 has three terminals with center one is ground and the rest of two are input and output. This regulator is chosen because it provides 5V for the microcontroller to work. Besides that, the regulator also gives 1A of current which is sufficient to be used in the circuit.

2.5.5 LM1117 Voltage Regulator

The Figure 10 and the table 4 shows the LM117 voltage regulator and its technical information.



Figure 10: Lm1117 3.3v Voltage Regulator



Table 4: Technical Information About Lm1117

Parameters	**Technical Information**
Input voltage	5V to 10V
Output voltage	3.3V
Output current	5mA
No of pins	3

The physical appearance of the LM1117 is similar to the LM7805. It has three pins with center pin to ground. The regulator supply 3.3V for the Bluetooth chip.

2.5.6 Relay

The Figure 11 and the table 5 shows the Relay used and its technical information.



Figure 11: Relay

Table 5: Technical Information About the Relay.

Parameters	**Technical Information**
Input voltage	5V to 220V
Support current	10A for AC and 10A for DC
Switching time	5μs
No of pins	5

Relay operates in the principle of electromagnetic induction. The relay has five terminals with two terminals are used to control the arm contact. The relay must be triggered using DC energy. Typical voltage suitable to trigger the relay is 5V to 220V.

The use of relay in the project is to control the opening and closing of the magnetic lock. One relay is for the magnetic lock and the other two is for the two status indicator lights.

2.5.7 Magnetic Lock

The Figure 12 and the table 6 shows the Magnetic lock used and its technical information.



Figure 12: Magnetic Lock (12volts)

Table 6: Technical Information About Magnetic Lock

Parameters	**Technical Information**
Input voltage	12V/24V
Current drawn	420mA
Holding force	500kgx2(1200Lbsx2)
Weight	3kg

The Magnetic lock used for this project is a small cabinet locker size magnetic lock

with low holding force and requires less voltage for operation. Though it cannot be used to fully implement the final product, it can be used to construct the prototype to analyze the concept of this project.

2.5.8 Liquid Crystal Display (16x2)

The Figure 13 and the table 7 shows the Liquid crystal display used and its technical information.



Figure 13: Liquid Crystal Display (16x2)

Table 7: Technical Information About Liquid Crystal Display

Parameters	Technical Information
Input voltage	5V
Current drawn	1.5mA
Operating temparature	15-50 Centigrate
No. Of pins	16

This is a basic 16 character by 2 line display. It displays Black text on Green background. Utilizes the extremely common HD44780 parallel interface chipset. Interface code is in the Appendix. Lastly, it includes LED backlight.

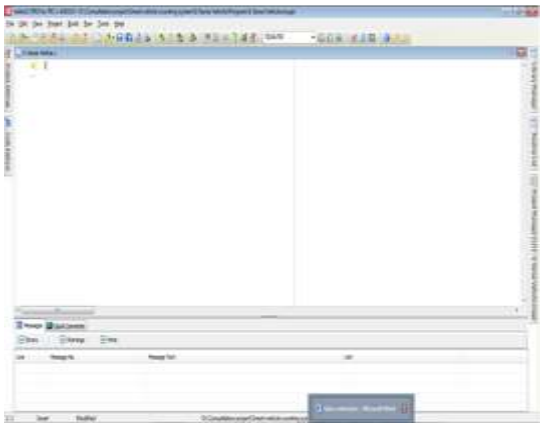


Figure 14: Mikro C Window

2.6 Software Tools

Apart from the hardware implementation, software tools are also important in implementing the project. The software's are used to write the program, simulate the circuit and designing the PCB layout. Below are the software used in the project:

2.6.1 Mikro C

Mikro C is a C language compiler specifically designed to program all 16Fxxx family types of microcontrollers. The compiler is developed by Microchip Company. It is free to download and use.
The reason of choosing MikroC is that it gives compilation speed faster than the MPLAB or other compiler. MikroC does not need include header files while programming is written. This is the special part of the MikroC. Thus, it shortens the programming language and easy to understand. Figure 14 shows the MikroC window.

2.6.2 Pickit2

PICKit2 is a software that is used to burn the Hex code or Hex file into the microcontroller. This software works together with the programmer kit. When any microcontroller loaded into the programmer, the PICkit2 will automatically detect the name of the microcontroller and shows it in the window. Figure 15 shows the PICkit2

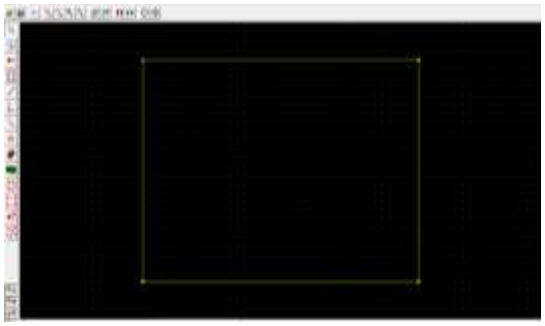
window.



Figure 15: Pickit2 Window

2.6.3 Express PCB

Express PCB is a CAD software. This software is used to design a schematic diagram and PCB. Express PCB is easy to learn with few steps and eliminate the complexity. Unlike DIPspace or ORCAD, the express PCB does not need to adjust the size of the PCB or schematic diagram. The software will automatically adjust according to the user circuit. Figure 16 shows the Express PCB window and express schematic window.



a) Express PCB window.



b) Express schematic window.

Figure 16: Express Pcb Window.

2.7 Circuit Simulation

Based on the block diagram shown in Figure 3, the circuit simulation is shown in Figure 17 using the PIC16F877A was simulated. A completely different microcontroller circuit was built from scratch, which acts as the android mobile phone for keying in the password or input signal because of the absence of a Bluetooth module or any wireless device in Proteus the android mobile phone circuit and the lock system circuit were connected using wires. The serial communication pin (Rx) was used as the input pin and port A, B and pin D0 were used as output port and pin. When the password is keyed in from the keypad, the relay gate is triggered to turn off if the password is correct or it stays on if the password is wrong also the status of the lock would be displayed in both LCD's depending on the keyed in password.

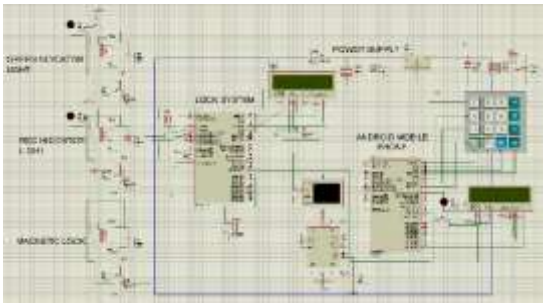
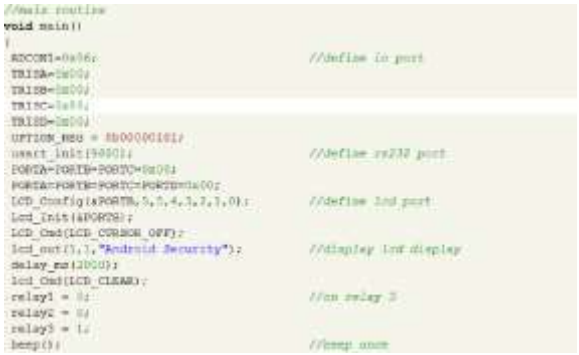


Figure 17: Proteus Circuit Simulation

2.8 Programing for PIC Microcontroller

The function of the circuit shown in Figure 17 is very much depends on the program design and embedded into the microcontroller. As seen in the flowchart, the general concept of the program has been explained. This section will show a complete C coding for the microcontroller to control the opening and closing of the magnetic lock when the Bluetooth module receives signals. The figure 18 shows the complete C coding to control the lock:



```
//main routine
void main()
{
 ADCON1=0x06;                          //define in port
 TRISA=0x00;
 TRISB=0x00;
 TRISC=0x80;
 TRISD=0x00;
 OPTION_REG = 0b00000101;
 usart_Init(9600);                     //define rs232 port
 PORTA=PORTB=PORTC=PORTD=0x00;
 PORTA=PORTB=PORTC=PORTD=0x00;
 LCD_Config(&PORTB,5,5,4,3,2,1,0);     //define lcd port
 Lcd_Init(&PORTB);
 LCD_Cmd(LCD_CURSOR_OFF);
 Lcd_out(1,1,"Android Security");      //display lcd display
 delay_ms(2000);
 Lcd_Cmd(LCD_CLEAR);
 relay1 = 0;                           //on relay 3
 relay2 = 0;
 relay3 = 1;
 beep();                               //beep once
```

Figure 18 Mirocontroller programming part1

As seen in the figure 18 is the main routine coding, The function begins with "void main()". This function is called embedded C program main body function. Inside the function, there can be multiple functions such as decision-making functions, infinite loop function, loop functions and I/O control functions. The Figure 19 shows the PIC controller used for the task.

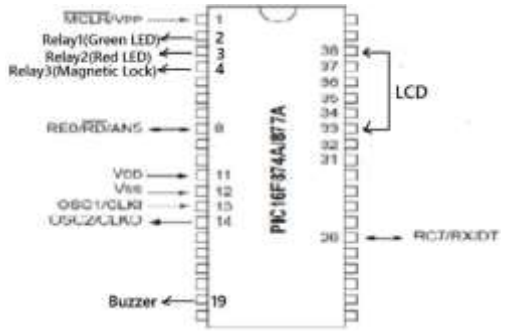


Figure 19: Pic16f877a Pin Configuration

ADCON1=0x06: this line of code is used to turn of analog to digital converter of port A and turn port A to a digital port.

TRISA = 0x00, TRISB = 0x00, TRISC = 0x80, TRISE = 0x00 this declares Port A, B and D as output ports respectively while pin 26 (RX pin) of Port C was declared as an input pin which is a neccessity for serial communication.

Next is the OPTION register configuration "**OPTION_REG = 0b00000101**" is a readable and writable register which contains various control bits to configure the TMR0/WDT prescaler, the external INT interrupt and TMR0. The binary configuration used means that it is set to prescaler 1:64 and timer 1.

The next line in the coding is **"USART_Init (9600)"** which initial the pin 25 and 26 and helps to define the RS232 port. These pins are reserve for data transmission and reception. Both of these pins have a standard data rate of 9600kbps.

In the next phase, portA,B,C and D are cleared and the LCD ports are defined using **"LCD_Config(&PORTB,5,5,4,3,2,1,0);"** Once the USART is initialized, then the command **"Lcd_Init(&PORTB);"** and **"LCD_Cmd(LCD_CURSOR_OFF);"** is to initialize the LCD in port B and turn of the blinking cursor.**"lcd_out(1,1,"Android Security")"** is used to display "ANDROID SECURITY" and there was a 2 second delay before the LCD was cleared. In the next commands, the relay 1 and 2 were turned of while relay 3 (magnetic Lock) was turned on: **relay1 = 0;, relay2 = 0;**, **relay3 = 1;**

The reason these is done is to set the lock system in its initial condition were the system is locked and both notification lights are turned off. The next command **"beep();"** is to give the buzzer a high

voltage so that it makes a beep sound notifying that the system is now turned on. The Figure 20 shows the part2 of the embedded programming code.

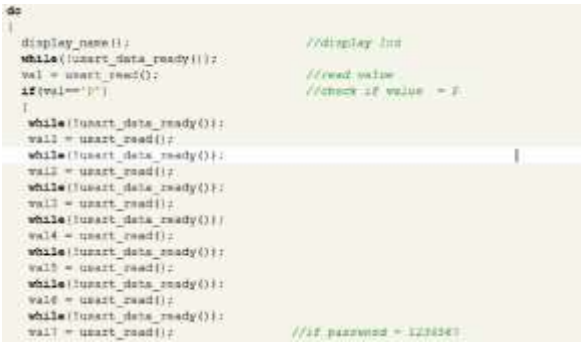


Figure 20: Microcontroller programming part2

The next command is "do{display_name();" is used to call upon the subroutine "displayname" to display on the LCD. Then

while(!usart_data_ready());
val = usart_read();
if(val=='P')
{

The next line of code simply means to set the microcontroller in a ready state to read any received data that has the header P followed by seven digits. The Figure 3.21 shows the part3 of the embedded programming code



Figure 21: Microcontroller programming part3

"if (val1=='1' && val2=='2' && val3=='3' && val4=='4' && val5=='5' && val6=='6' && val7=='7')"

The code in quote above means if the Password is "1234567" and having the header P then the relay 2 and 3 should be in off state while 1 should be off. But in a case were the password is incorrect, the relay 2 and 3 would be in on state while relay 1 would be off.

The signal detection continues or starts over again from the while(1) function. The detection of input signals from Bluetooth is non-stop until the power supply of the microcontroller is cut off.

2.9 Circuit Constructed on Breadboard

The Figure 22 shows the breadboard prototype of the designed task.

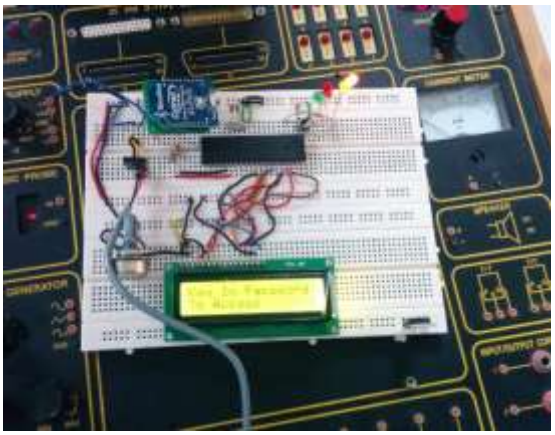


Figure 22: Circuit Constructed On Breadboard

A simple Bluetooth control circuit is constructed on breadboard and prepare for testing. Although the Bluetooth module has many pins, only the Vcc, ground, input and output pins were used. During the testing process it was noted that the bluetooth module is very sensitve to its input voltage (3.3volts). A voltage greater or less than 3.3volts would result in irregular data transmission. The Figure 23 show the prototype power supply on a

breadboard.

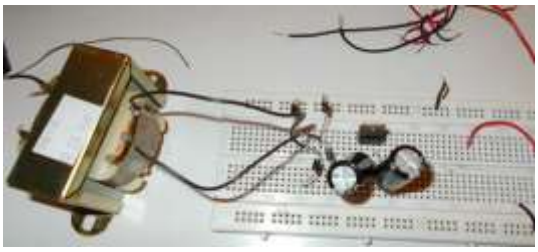


Figure 23: Power Supply Circuit

2.10 PCB making

Once the circuit and program tested successfully, the next step of doing the project is PCB making. The PCB making involves PCB layout design, printing, ironing and etching. All of these steps will be briefly explained in this section. Figure 24 shows the PCB layout design.

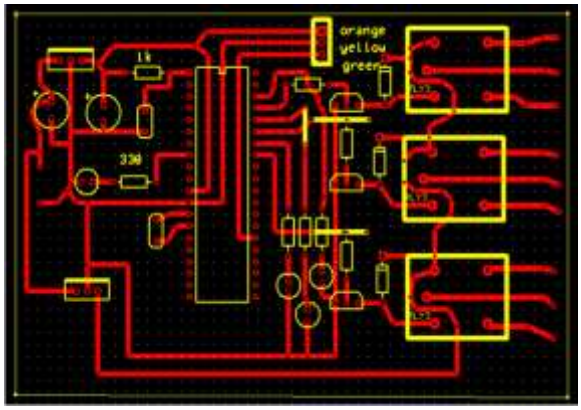


Figure 24: PCB Layout Design for the Bluetooth Receiver

The design of PCB layout will consider two issues: one is open circuit and the other is short circuit. The open circuit will not have current flows in the circuit. Thus, there will be no response at the output.

Short circuit will result heavy current flows in the circuit. This is very dangerous because it can damage most of the electronic components. In the worst case, fire accident may result.

Open and short circuit can be checked through the software or print the layout on the surface of the PCB board.

Once the PCB layout has been designed, the layout is then printed out using laser printer. Figure 25 shows the laser printer used to print out the PCB layout.



Figure 25: PCB Layout Print Out

The reason to use laser printer to print out the PCB layout is because of:

1. In the ironing process, the image of layout is easily transfers to the PCB copper board.
2. The layout can withstand high temperature.
3. The layout can withstand high concentration of acid solution.

When the layout is printed out, the next step is ironing. Ironing is a process of heating. It uses heat to transfer the image of printout on the PCB board.

Figure 26 shows the ironing of PCB board using a pouch laminator.



Figure 26: Ironing

Next after ironing is a chemical etching. Etching is a process of removing the unwanted areas of the copper board. Etching requires acid called iron (III) chloride. Figure 27 shows the PCB board

prepares for etching. Figure 28 shows the PCB board after etching.



Figure 27: Prepare For PCB Etching

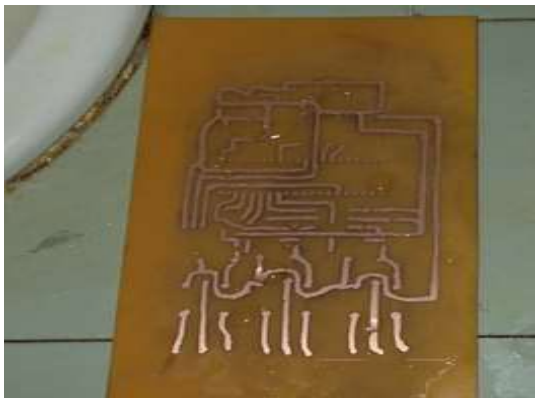


Figure 28: PCB Board After Etching And Clean

2.11 Prototype testing

Figure 29 shows the testing of the prototype with the smart phone (LG Nexus 5) acts as a controller.

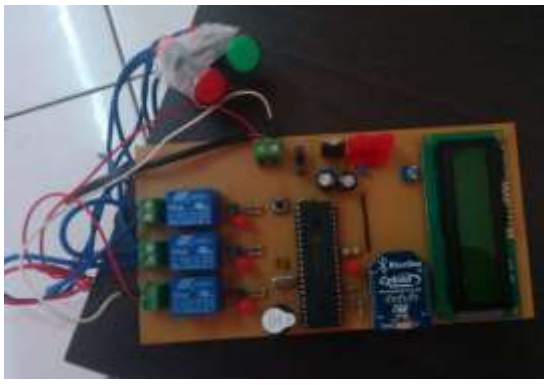


Figure 29: Prototype Under Testing

Figure 29 shows the working of the entire project. Note that operation is simple and can be summarized as shown below:

- Turn ON the smart phone.
- Access into Bluetooth GUI apps.
- Turn ON the Bluetooth by clicking “connect”.
- Switch ON the control board by connecting it to 220V power source.
- Key in Password in Android mobile phone to turn OPEN Lock.
- The Lock system should response according to the keyed in Password.

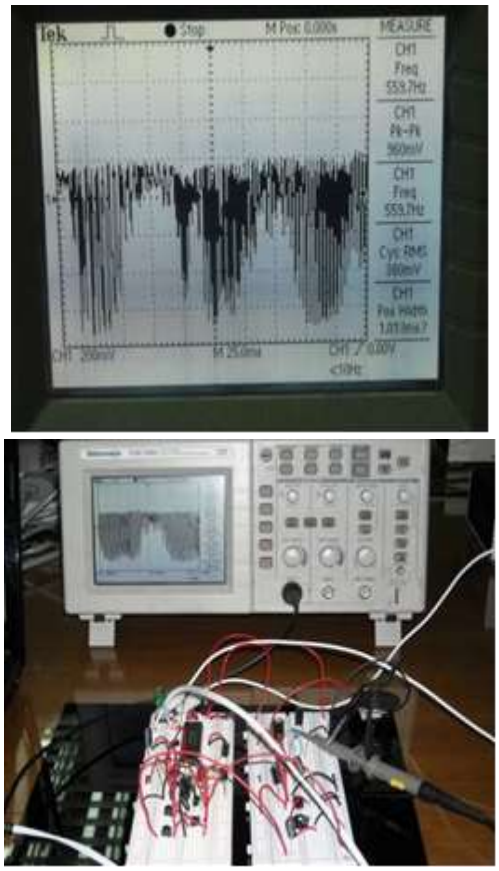
The possible errors which might happen to the prototype when it is connected to power source are listed below:

- The Bluetooth chip does not show the blinking LED light – try to restart the whole control board. This happen because the microcontroller cannot catch the transient voltage.
- The Bluetooth in the phone not pairing – try turn OFF and ON the circuit.
- The Bluetooth at the phone does not show Bleu BEE – try to restart the control board.
-

3 RESULT AND DISCUSSION

This section presents the experimental test carried in the lab. The section will show the breadboard testing results, analysis of the results and present the final outcome of the prototype. The instruments used to perform the testing are multimeter and oscilloscope.

3.1 Breadboard testing



(a) Measuring the Bluetooth signal. (b) Enlarge Bluetooth signal.

Figure 30: Measuring The Bluetooth Signals

The Bluetooth testing in the case shown in Figure 30 is in the noisy environment. As seen in the diagram, the received signal is distorted. The data rate cannot be measured because of the oscilloscope constraint. Table 8 shows the experimental observation on the output of the Bluetooth chip when transmission happens in ten times.

Table 8: Experimental Test To Observe The Output Of The Bluetooth Chip

No. of experiment	**Output voltage (mV_{pp})**
1	960
2	730
3	850
4	770
5	830
6	650
7	720
8	880
9	945
10	721

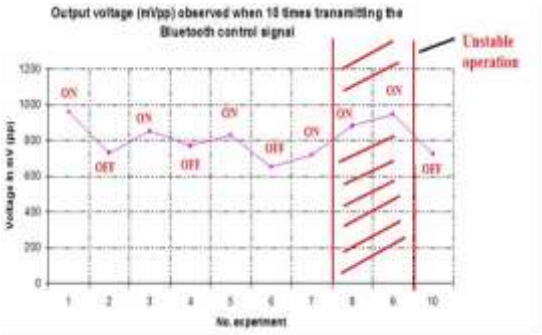


Figure 31: The Plot for Table 9

Notice that in Figure 31, when experimental test to key in password in the smart phone to control the lock, it was found that at the seven to nine times experiments the system works unstable. During this period of time, the relay gate ON all the times and it never goes OFF or move in.

When analyzing the results, it was observed that the Bluetooth chip lost the connection from the smart phone transmitted Bluetooth signal. This happen because the receiver circuit gets overheated due to relays drawing too high current.

3.2 Bluetooth signal plot

The gate remote control software built in the Xperia hand phone. Table 9 shows the experimental test on maximum distance that the Bluetooth signal can transmit.

Table 9: Experimental Test of Bluetooth Signal Strength

No of ex-periment	Output voltage (mVpp)	Distance (m)
1	960	1
2	845	2

3	730	3
4	660	4
5	543	5
6	489	6
7	330	7
8	300	8
9	202	9
10	150	10
11	88	11
12	73	12
13	43	13
14	31	14
15	20	15
16	15	16
17	6	17
18	0	18
19	0	19
20	0	20

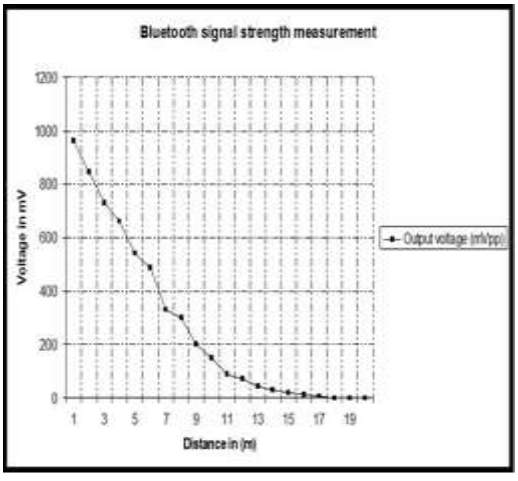


Figure 32: The Plot for Table 9

As seen in Figure 4.3, the longer the distance travelled, the lower the signal is. The Bluetooth signal varnish after 20m from the receiver. Under that distance, the signals drop badly and almost to zero.

By looking into the exponential decay graph shown in Figure 4.3, the solution to describe such graph is:

$$y(x) = ce - kx \quad (5)$$

When substitute x = 1 or v(1), the expression become:

$$y(1) = 960mVe - k \quad (6)$$

Thus, the general expression for the graph shown in Figure 5.4 is:

$$y(x) = 960e - kxmV \quad (7)$$

Where k is a constant, x is the distance. By differentiating the v(x) with respect to x, we have:

$$\frac{dv(x)}{x} = -960ke^{-kx}mV \quad (8)$$

4 CONCLUSION AND RECOMMENDATION

The Android Lock System using Bluetooth was successfully implemented. Although a 12volt magnetic lock was used for the project giving the lock magnet a low holding force of 1200Lbs making it easier for it to be pulled apart. The Bluetooth pairing of the two transceivers (i.e. the transmitter and the receiver) depends on the distance at which the two transceivers are, the signal is stronger at close range and gets lower and lower as the distance increase, there will be a total reception lost at a far distance between the transceivers.

Although it was a class 3 Bluetooth Bee

module, the maximum distance reach between the transmitter and the receiver must be at least 20 meters.

However, for future improvement, the system can also be implemented on ordinary phones of any operating system other than android smart phone and also the Bluetooth Bee module distance for a class 3 Bluetooth devices can be improved to 100 meters. Also, the 220 volts magnetic lock should be used for the system to give it a greater holding force that can withstand any force from pulling apart the two sides of the magnetic lock.

In the android mobile phone application side, it was designed to simple act as a way to key in the password and the data transferred to the microcontroller via Bluetooth were the password is compared to access whether it is correct or not but in future in improvements, the application could be built is such a way that all data comparisons are done in the mobile application before the data is transmitted to the microcontroller and also an implementation of a self-lock system in the application could be made whereby the application locks itself for a particular amount of time after the wrong password has been keyed in three consecutive times.

REFERENCES

Abbas, M., Khan, S. A., & Ali, S. (2025). Double-layered authentication door-lock system utilizing hybrid RFID-PIN technology for enhanced security. *Engineering Proceedings*, 23(1), 19.

Almheiri, S., & Alblooshi, M. (2023). Exploring the efficiencies and vulnerabilities of smart door control systems: A systematic review. In *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1–6). IEEE.

Al-Shammaa, A. R., & Al-Majidi, S. D. (2013). Real time smart home automation based on PIC microcontroller, Bluetooth and Android technology. *International Journal of Engineering Research & Technology (IJERT)*, 2(12), 2115–2120. https://www.ijert.org/research/real-time-smart-home-automation-based-on-pic-microcontroller-bluetooth-and-android-technology-IJERTV2IS120765.pdf

Arredondo Balboa, H. B. (2013). *Implementación de un sistema de domótica para aplicación Android vía Bluetooth con microcontrolador PIC 16F877A* [Implementation of a home automation system for Android application via Bluetooth with PIC 16F877A microcontroller] (Tesis de pregrado). Universidad Mayor de San Andrés, La Paz, Bolivia.

Felix, C., & Raglend, I. J. (2011). Home automation using GSM. In *2011 International Conference on Signal*

Processing, Communication, Computing and Networking Technologies (ICSCCN) (pp. 15–19). IEEE.

Mahajan, M., & Khadse, S. V. (2020). Home automation using Bluetooth. *International Journal of Engineering Research & Technology (IJERT)*, 9(4), 455–458. https://www.ijert.org/research/home-automation-using-bluetooth-IJERTV9IS040258.pdf

Pannirselvam, D. H., & Zohari, M. H. (2025). IoT-enabled dual authentication system using RFID and passcode for college dormitories. *Progress in Engineering Application and Technology*, 6(1), 1–10.

PIC Microcontroller. (2017). Electronic code locking system using PIC 16F877 microcontroller. *PIC Microcontroller Projects*.

Quispe, G., & Mamani, C. (2023). Development of a microcontroller-based smart front door lock system. In *2023 7th International Conference on Smart Technology (ICST)* (pp. 1–5). IEEE.

Rathnayaka, A. J. D., Potdar, V. M., & Kuruppu, S. J. (2011). Evaluation of wireless home automation technologies. In *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (DEST 2011)* (pp. 76–81). IEEE.

Sanchez, A., & Martin, J. (2024). Research on smart-locks cybersecurity and vulnerabilities. *Wireless Networks*, 30, 5905–5917.

Sriskanthn, N., Tan, F., & Karande, A. (2002). Bletooth based home automation system. *Microprocessors and Microsystems*, 26(6), 281–289

Theint, M. S. S., Soe, M. T., Mon, A., Maung, L. M. M., & Shein, S. H. H. (2026). GSM based door lock security-controlled system with microcontroller. *Journal of Engineering Technology and Applied Physics*, 8(1), 1–5.