International Journal of Engineering & Technology, 9 (2) (2020) 480-486

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Design and implementation of access door control with mobile alert

Chijioke Nwogu [1], Monday Eze [2] *, Charles Okunbor [1]

[1] College of Postgraduate Studies, Babcock University, Ogun State, Nigeria
[2] Department of Computer Science, Babcock University, Ogun State,
**Corresponding author E-mail: ezem@babcock.edu.ng*

Abstract

The necessity for adequate security of lives and properties cannot be overemphasized. Tackling insecurity in an effective manner calls for active computer-based research and solutions. Essentially a security system is designed to help detect intrusion and prevent unauthorized access. These security threats are tracked by installing various security access doors and alarm systems. Findings have shown that many access doors use either password or biometric forms of authentication separately which are easily compromised. This paper presents a two level automated access control for door security with mobile alert system, powered by a 5V, 6000mAH battery. In addition a multi-factor authentication using biometrics (fingerprint) and password was also used to enhance access control for this system. A mobile phone call alert and alarm system was uniquely included to this design to notify owners of the presence of an intruder when multiple attempts of incorrect login credentials are presented to the system over a short period of time. The program for the microcontroller was written in C language. This paper concluded that the use of multi-factor authentication with mobile phone alert will help improve the security for access doors used in banks, residential buildings, hospitals, military installations and other institutions, especially where confidentiality and restrictions are needed.

Keywords: *Access Control; Authentication; Intrusion Detection; Fingerprint; Mobile Alert; Security.*

1. Introduction

The essence of access control doors is to restrict unauthorized persons to a building or office. Access control for many years was at the mercy of deadbolt, pad locks and matching brass keys [1]. These locks have proved to be inadequate, because breaking the pad locks is quite easy. In the recent times however, computer-based electronic access control system has provided a convenient platform to authorized persons while denying access to unauthorized ones. Essentially a security system is designed to detect intrusion, unauthorized entry into a building or a protected area and denial of unauthorized entry in order to protect households and properties from damage or harm [2]. Security systems are found in residential, commercial, industrial and military installations for protection against theft, damages, as well as personal protection against intruders. With the introduction of Global System for Mobile Communication (GSM) and mobile smart devices with high computing power, this research seizes the opportunity to increase the security of access control doors with multi-factor authentication using password, fingerprints and mobile phone call alert system [3]. The main objectives of this research are to:

i) Construct a device that utilizes numeric code and fingerprint module to allow access,
ii) Provide a code for activation and deactivation process, and a friendly user interface for effective and round the clock monitoring against intruders.

This research is significant because multi-factor authentication has proven to provide better access control mechanism for security systems. Older security methods using radio frequency identification (RFID) cards and key locks have proven less secure because RFID cards [4] and key locks can be cloned and stolen.

2. Related works

Surveillance of homes has been made easy by the manufacturers of home security alarm and monitoring systems, as various methods are made available for users to keep a watch over their homes, even when they are on tour or at work place. Recent among the alarm technologies is the paging system which can notify the owners through the changes in the alarm system. Though this development in technology is a welcomed advancement, it is yet not the final solution to home security needs [5].

A research [6], designed an access control system using a one-time password (OTP) to make up the gaps of the user authentication mechanism such as mechanical door-lock. The system user must register a mobile phone and know how to use the OTP which is generated and sent to the user's mobile phone [7] whenever the user requests to gain entrance to the facility. However, this form of door access control is

Copyright © Chijioke Nwogu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

deficient because it is not multi factor authentication-based and users are not notified when unauthorized users try to gain access into the facility.
Furthermore, [8] presented a paper titled "Password protected electronic lock system for smart home security". The system uses a keypad, 16 x 2 Liquid crystal display (LCD) and a PIC18FA52 microcontroller [9] which enable users to get notification of an intruder on their LCD. This current work is an enhancement, as it introduces a multi-level authentication and a mobile phone alert to notify users irrespective of their location.
A Radio Frequency Identification (RFID) and password based system using Arduino UNO was proposed by [10]. RFID reader is used to read the value on the RFID ID card and the Arduino UNO. If the ID card is true, Arduino enables password to be pressed on keypad. If password is true, lock style solenoid is unlocked, but if false, solenoid is locked. Though the work used a two factor authentication, it can be compromised if the password is leaked and the RFID ID card falls into a wrong hand, quite unlike the current work.

3. System design

The design of this access control system is broken down into the following modules:

3.1. Fingerprint

The SM630 fingerprint module gets and stores the fingerprint [11] of users and compares the stored fingerprint with that of an intending user. Table 3.1 shows the available command codes. If there is a match, it sends signal to the microcontroller to grant access to the user. The fingerprint module is connected to the microcontroller through its serial communication pins.

Table 3.1: Command Codes for Fingerprint

S/N	Name of Command	Command Codes
1	Add Fingerprint	0x40
2	Delete Fingerprint	0x42
3	Search Fingerprint	0x44
4	Empty Fingerprint Database	0x46
5	Search Information in Fingerprint Database	0x4B
6	Download Fingerprint Template	0x50
7	Upload Fingerprint Template	0x52
8	Read ID Number	0x60
9	Read User Flash	0x62
10	Write User Flash	0x64
11	Read Product Logo	0x80

3.2. The keypad

The keypad consists of pull up/down resistors and the push button. The controller is programmed such that the code input keys normally sends a HIGH (5V) to its keypad pins. In this state, the microcontroller does nothing but scan the key input for a change of state from HIGH to LOW. When there is a LOW from the key, the microcontroller executes its instruction according to when and where the input signal was received. To make the code input send a normally high signal to the controller, pull up resistors are employed. The value of the resistor used was derived thus:

From Ohm's Law: $V_{cc} = I_P R_P$ (1)

where I_P is the current through the pull up resistor and R_P is resistance of the pull up resistor. To avoid over heating of the resistor and also to minimize the current consumption of the system, a current of 0.5mA was designed to flow through the pull up resistor [12] to the microcontroller. Hence from (1);

$$R_p = \frac{V_{cc}}{I_p} \quad (2)$$

$$= \frac{5}{0.5\times10^{-3}}$$

$= 10K\Omega$.

Therefore, $R_4, R_5, R_6, R_7, R_8, R_9, R_{10}, R_{11}, R_{12}, R_{13}$ of $10K\Omega$ were used.

3.3. Display circuit

The display section of the circuit consists of a Liquid Crystal Display (LCD). The liquid crystal display [13] used is the HD44780 LCD. Its displays the time as rendered by the real time clock (RTC) and also performs the user interface function. The LCD needs a 5V source of power for operation and to power the internal light emitting diode [14] in the LCD screen which serves as the backlight of the LCD. The data pins of the LCD (D0-D7) are connected to the microcontroller through port P3 as shown in Fig. 3.1. The microcontroller displays the information on the LCD by sending a high logic level (2.2V to 5V) or low logic level (0V to 0.6V) to each of the data pins of the LCD as specified by the datasheet for the HD44780 LCD.

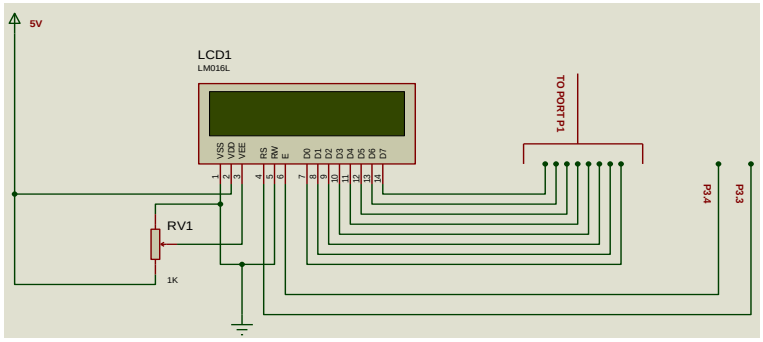


Fig 3.1: LCD Display Circuit Diagram.

The HD44780 LCD has two built in registers namely data register and command register [15]. Data register is for placing the data to be displayed and the command register is to place the commands.

3.4. Door mechanism

The door mechanism consists of L293D bidirectional motor drive, dc motor and sliding door. Fig. 3.2 is the circuit diagram [16] of the door mechanism.

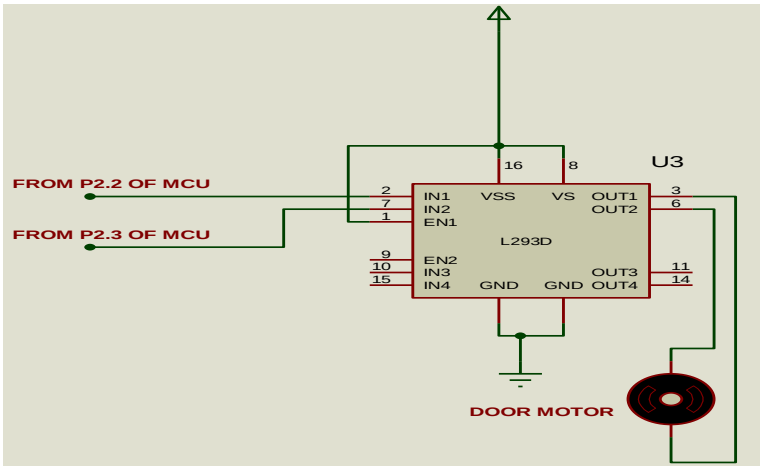


Fig. 3.2: Door Mechanism Circuit Diagram.

The L293D device is a quadruple high-current half-H driver designed to provide bidirectional drive currents [17] of up to 600-mA at voltages from 4.5 V to 36 V. It is designed to drive inductive loads [18] such as relays, solenoids, DC and bipolar stepping motors, as well as high-current/high-voltage loads in positive- supply applications. The microcontroller through its P2.2 and P2.3 sends input to the motor drive. When input to the L293D IN1 is HIGH, the motor rotates in the clockwise direction and when input to IN2 is HIGH, the motor rotates anticlockwise.

3.5. The alarm circuit

The alarm circuit is made up of mobile alert, audio and visual alert as shown in Fig. 3.3.

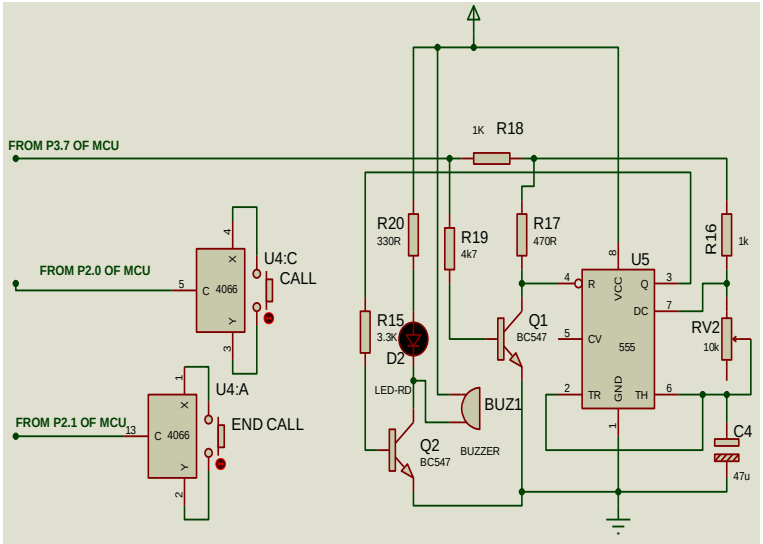


Fig. 3.3: The Alarm Circuit Diagram.

3.5.1. Mobile alert

The mobile alert circuit consists of a mobile phone (Nokia C102) with a network sim card and electronic switch CD4066. The mobile alert [19] utilizes the electronic switch CD4066 IC to dial the last dialed phone number on the mobile set and after some time, it also ends the call. After a careful study of the Nokia C102 and the mobile networks in Nigeria, it was found out that;

a) At the mobile phone sleep mode, it takes four call keypad operations to call the last dialed number in the phone call log.
b) Some mobile networks prompt user (caller) to drop a voice record message to an unreached receiver when the line has rang for a long time without picking up. This voice record message consumes air time.

The CD4066 is a low input current consuming device [20] hence, the current from P2.0 and P2.1 of the microcontroller is sufficient to connect both pins to the control pins 5 and 13 of the CD4066 respectively as showed in Fig. 3.3.
A HIGH of 0.5second duration is sent four times to the control pin 5 of CD4066 from the microcontroller P2.0, which causes the CD4066 to operate its U4:C switch and since the mobile call key is connected to this switch, the call key is also operated four times thus, a call is made to the last dialed number in the call log. The call needs to end before it gets to the voice record prompt so as not to waste air time since this project uses the mobile network as an alert (flash) medium.

It was observed that none of the major Nigeria mobile networks such as MTN, Glo, Airtel and 9mobile prompts for voice record message less than 15 seconds after initiating a call. Therefore they end the call after 15 seconds of call initiation and as at this time, the call may have gone through and already rang for some seconds. To end the call, the microcontroller sends a HIGH of 0.5second duration once to the CD4066 control pin 13 , which causes the CD4066 to operate its U4:A switch and again since the mobile call-end key is connected to this switch, the call-end key is also operated once thus, the dialing call is ended. After the end call, there is a delay of 3 seconds before another call is again initiated. This dial and end-call continues indefinitely until a hard/soft reset is made to the system. It should be noted that the mobile phone is not shown in the circuit diagram, however the call and call-end buttons are represented with the CD4066 switch contact terminals as shown earlier in Fig. 3.3.

3.5.2. Audio circuit

The audio circuit is made up of NE555 IC, buzzer, resistors, switch, capacitor and NPN transistor BC547. The NE555 is configured in "astable" mode at a frequency of 1.5Hz. This frequency is chosen in order to give the alarming effect of sound and also to give a dimming effect of light. The values of the capacitor and resistors [21] are derived as follows;
From NE555 data sheet,

$$F = \frac{1.44}{(R_A+2R_B)\times C} \quad (3)$$

Where F is frequency in Hz,
$R_{A,}$ R_B are resistances in Ω and
C is capacitance in Farad, F.
To get a frequency of 1.5Hz, a resistance value of 1kΩ for R_A=R_{16} and capacitor C=C_4 value of 4.7uF were chosen. Hence, the value of R_B

= R_{v2} can be calculated as follows;

$$R_{v2} = \frac{1.44-F\times C4\times R16}{2FC4}$$

$$= \frac{1.44-1.5\times47\times10^{-6}\times1\times10^{3}}{2\times1.5\times47\times10^{-6}}$$

= 9.713kΩ

R_{v2} of 10kΩ was used and was varied to 9.713kΩ.
Therefore, the output pin 3 of the NE555 outputs 3.5V at a frequency of 1.5Hz. This output is used to drive the base of transistor Q2 and in turn drive the buzzer and the red LED D5.
A base current of 1.1mA is enough to drive the Q2 to saturation. The base resistor R_{15} is calculated thus;
Applying Kirchhoff Voltage Law to the base circuit,

$V_{bb} - I_bR_{15} - V_{be} = 0$,

Where V_{bb} is the base voltage= output voltage from the "astable" circuit [22], V_{be} is the base emitter voltage of Q=0.7V, I_b is the base current = 1.1mA.

$$R_{15} = \frac{3.5-0.7}{1.1\times10^{-3}}$$

=3.182kΩ

Hence R_{18} 3.3kΩ was used.
At saturation, V_{ce} = 0v
For adequate illuminance, a current of 11mA=I_{20} was designed to pass through the red LED D2. At 11mA the forward voltage drop [23] of red LED is 1.5V,

$$V_{CC} - V_D - I_{20}R_{20} = 0 \quad (4)$$

$$R_{20} = \frac{V_{cc}-V_D}{I_{20}}$$

$= \frac{5-1.5}{11\times10^{-3}}$

=318.2Ω.

Therefore, R_{20} = 318Ω.
As can be seen from Fig. 3.3, the buzzer is also connected in series to the collector. This enables it to buzz at a frequency of 1.5Hz.
The pin 4 of NE555 is the reset button. A LOW in this pin disables the oscillating circuit while a HIGH enables the oscillating circuit. Normally, a HIGH is sent from P3.7 of the microcontroller to the base circuit of Q1 which causes the saturation of the transistor [24] and therefore bringing the reset pin 4 to a LOW. When there is an intruder in the system, P3.7 sends a low to the base circuit of Q1 hence, the transistor will be in cut off mode. This makes the reset pin 4 to be pulled up through R_{17} to a HIGH and hence, the circuit oscillates.

3.6. System flowchart

The flowchart for this system is shown in Fig. 3.4

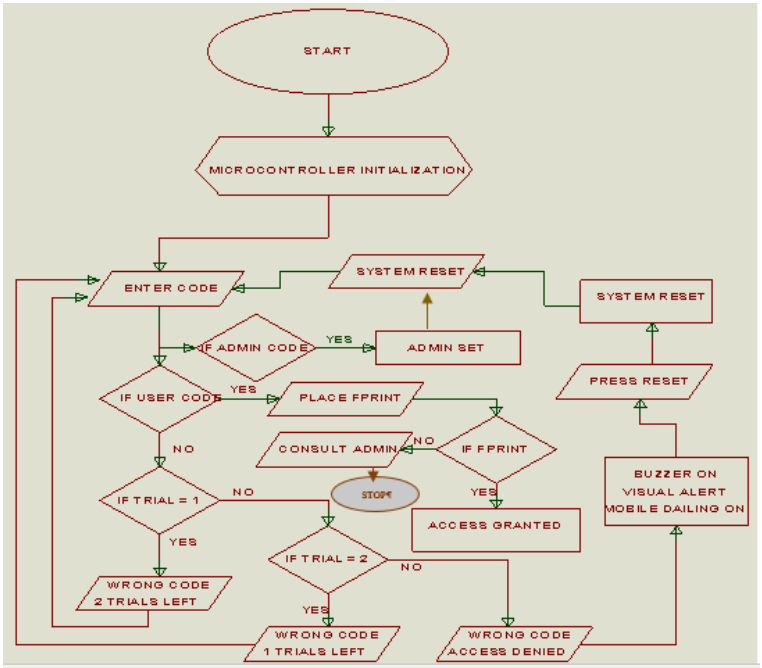


Fig. 3.4: Flowchart for the Door Access Control System.

4. Implementation and result

The following section shows the outputs displayed at different stages, sequel to the implementation and testing of this work.

4.1. Authentication

To gain entrance, power on the safe box and wait for the home screen to display “PRESS ENTER”. To login at this time press enter key until it displays ‘‘ENTER CODE’’. Fig, 4.1 shows the LCD screen waiting for a user to enter a code. Input the user code (which is a combination of digits from 1-4), then press the enter key. After pressing the enter key, it prompts the user for fingerprint scanning. This is the first level of authentication. Fig. 4.2 shows the LCD display of access granted when the correct password is entered into the system and is prompted for a second level authentication using fingerprint.



Fig. 4.1: LCD Display to Enter Code.



Fig. 4.2: Output for Access Granted.

When the wrong code is entered three (3) times, access is denied to the user wanting to gain access and the system is locked. This also triggers the alarm system and also puts a call across to a registered administrator to notify him or her of an intruder. Fig. 4.3 displays the output of the LCD when a wrong code is entered.

4.2. Fingerprint registration

To register a fingerprint for biometric authentication, press admin key until "ADD NEW FPRINT'' is displayed as shown in Fig. 4.4, then press enter key when ''PRESS ENTER'' is displayed. After pressing the ENTER key, place the new user right thumb on the screen (fingerprint module) to capture the finger print. After adding fingerprint press reset to go back to home screen.



Fig. 4.3: Access Denied.



Fig. 4.4: Fingerprint Registration Display on LCD.

4.3. The microcontroller programming

The program for the microcontroller was written in C language. The keil µVision 4 software was used to compile the source code to Hex code (base 16 machine language). TOP2011 burner was used to write the Hex code to the AT89C52 microcontroller [25].

5. Conclusion

The two level security system implemented in this research consists of the password (or code) and the fingerprint. This system allows only authorized person to have access into the secured apartment or office after the password and fingerprint had been verified by the system. Thus, this work involves the simultaneous use of two level securities. It is fully controlled by the AT89C52 microcontroller. The password is stored in an EEPROM [26], interfaced to the microcontroller. Any attempt to open the door by entering the wrong password, an alert is actuated, indicated by a caution lamp and siren. This paper further enhanced door access control by interfacing a GSM modem [27] to the system so that when a wrong password is entered, a call is sent to the administrator or a concerned authority. Finally, the design and construction of a two level automated access door with mobile alert is an improvement over a number of other past research works in this area.

References

[1] Neelam M., Ruhinav H. and Priyanka B. (2016), Automatic Door Locking System. International Journal of Engineering Development and Research.Vol 4 (1), 495-499.
[2] Hossain, M. K., Biswas, P., Mynuddin, M., & Morsalin, S. (2014). Design and implementation of smart home security system. International Journal of modern embedded system, 2(6), 7-10.
[3] Wong D., Jones E. and Rubin G. (2018). Mobile Text alerts are an effective way of communicating emergency information to adolescents: Results from focus groups with 12 to 18 years olds. Journal of Contingencies and Crisis Management. Vol 26, 183-192. https://doi.org/10.1111/1468-5973.12185.
[4] Mandeep K., Manjeet S., Neeraj M. and Parvinder S. (2011). RFID Technology Principles, Advantages. Limitations and Its Applications. International Journal of Computer and Engineering Vol3. No1, 1793-8163.
[5] Lamberti, F., & Demartini, C. (2003). Low-cost home monitoring using a Java-based embedded computer. In 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, 2003, 342-345. https://doi.org/10.1109/ITAB.2003.1222549.
[6] Shin, S. S., Han, K. H., & Jin, K. Y. (2013). Digital Door Lock on the Access Control System using OTP-based User Authentication. International Journal of Digital Content Technology and its Applications, 7(11), 436. https://doi.org/10.4156/jdcta.vol7.issue11.56.
[7] Mohsen G. and Satar G. (2016). One-time password via SMS. *Bulletin de la Societe Royale des Sciences de Liege*, Vol 85, pp106-133.
[8] Rahman, M. M., Ali, M. S., & Akther, M. S. (2018). Password Protected Electronic Lock System for Smart Home Security. International Journal of Engineering Research & Technology, 7(4), 541-544.
[9] Altaf H, Muhammad H., Kamran H. and Tabinda Z. (2016). Programming a microcontroller. International Journal of Computer Applications. Vol 155 (5), 21-26 https://doi.org/10.5120/ijca2016912310.
[10] Hilang S. & Lwin S. (2019). Electronic Door Lock using RFID and Password Based on Arduino. International Journal of Trend in Scientific Research and Development, 3(2), 799-802 https://doi.org/10.31142/ijtsrd22875.
[11] Oloyede M., Adedoyin A. and Adewole K. (2013). Fingerprint Biometric Authentication for enhancing Staff Attendance System. International Journal of Applied Info. Systems. 5 (3), 19-24 https://doi.org/10.5120/ijais12-450867.
[12] Boasheng Y., Honhmei L. and Xiaoling Y. (2012). Logic Conversion Method in Serial Data System, Procedia Engineering 29 (2012) pp1539-1543. https://doi.org/10.1016/j.proeng.2012.01.169.
[13] Haiwei C. and Shin-Tson W. (2019). Advanced Liquid Crystal Display with Supreme Image Qualities. Journal: Liquid Crystals Today. 28 (1), 4-11. https://doi.org/10.1080/1358314X.2019.1625138.
[14] Samuel E. and Chukwuebuka E. (2018). Numerical simulation: controlling light emitting diodes from MATLAB. International Journal of Computer Aided Engineering and Technology, 2018, 10 (6), 748 – 761. https://doi.org/10.1504/IJCAET.2018.095212.

[15] Jagadal SB and Halse SV. (2012). Interfacing 8051 Microcountroller with LCD Using Multi Simulator. Journal of Computer and Mathematical Sciences, 3 (5), 498-556.
[16] Lakshman N., Dinesh R, and Prabhanjan S. (2019). Handwritten Electric Circuit Diagram Recognition: An Approach Based on Finite State Machine. International Journal of Machine Learning and Computing, 9 (3), 374-380 https://doi.org/10.18178/ijmlc.2019.9.3.813.
[17] Dong-Min L., Seung-Wook H., Jin-Wook K. Yong-Su N. and Chung-Yuen W. (2018). A Control Strategy for Bidirectional Isolated 3-Phase Current-Fed Dual Active Bridge Converter. Electronics 2018, 7 (214), 1-22. https://doi.org/10.3390/electronics7100214.
[18] Abhinav S., Saleem K., Shavet S., Parveen L. (2013). Dependence of Power Factor on Inductive Loads for Microcontroller based Power Systems. IOSR Journal of Electrical and Electronics Engineering. 7 (2), 30-35 https://doi.org/10.9790/1676-0723035.
[19] Sankari A. and Umasankar. K. (2013). Ensuring Security in Emergency through SMS Alert System. Int. Journal of Com. Appl. Tech. and Research. 2 (4), 487 - 491. https://doi.org/10.7753/IJCATR0204.1017.
[20] Yi-Tui C. (2017). The Factors Affecting Electricity Consumption and the Consumption Characteristics in the Residential Sector—A Case Example of Taiwan, Journal of Sustainability 2017, 9 (1484), 1-16. https://doi.org/10.3390/su9081484.
[21] Elton M. (2017). Analyzation of the Resistor-Inductor-Capacitor Circuit. Undergraduate Journal of Mathematical Modeling: One + Two, 7 (2), 1-19. https://doi.org/10.5038/2326-3652.7.2.4876.
[22] Moyeed A. (2017). Design and Implementation of Astable Multivibrator using 555 Timer. IOSR Journal of Electrical and Electronics Engineering. 12 (1), 22-29. https://doi.org/10.9790/1676-1201022229.
[23] Ming Y., Ziping C. and Jun L. (2018) Characterization the influences of diodes to piezoelectric energy harvester, International Journal of Smart and Nano Materials, 9 (3), 151-166. https://doi.org/10.1080/19475411.2018.1454532.
[24] Szafranek BN, Fiori G, Schall D, Neumaier D, and Kurz, H (2012). Current Saturation and Voltage Gain in Bilayer Graphene Field Effect Transistors. Nano Lett. 2012, 12 (3), 1324-1328. https://doi.org/10.1021/nl2038634.
[25] Yongxian S. (2011). Design of LED Display Control System Based on AT89C52 Single Chip Microcomputer. Journal of Computers, 6 (4), 718-724 https://doi.org/10.4304/jcp.6.4.718-724.
[26] Rahman, L., Ibne R. and Ali, MA. (2011). A low voltage-type sense amplifier design for EEPROM memory. Telecommunications and Radio Engineering, 70(15), 1379-1385. https://doi.org/10.1615/TelecomRadEng.v70.i15.80.
[27] Rozita T., Addin S., Kok W., Chan, M. and Vee H. (2013). Smart GSM Based Home Automation System. IEEE Conference on Systems, Process and Control (ICSPC 2013), Kuala Lumpur Malaysia, 2013, 306 – 309.