http://fepi-spas.com/spasjournal Article

Design of A Hybridized Security Door System with Password-Based Access and SMS Notification

[1*]Ehiagwina, F. O., [2]Olaiya O. O.
[1]*Department of Electrical/Electronic Engineering, Federal Polytechnic Offa, Offa, Kwara State, Nigeria*
[2]*Department of Computer Engineering, Federal Polytechnic Ilaro, Ogun State, Nigeria*
[1*]frederick.ehiagiwna@fedpoffaonline.edu.ng; Orcid ID: https://orcid.org/0000-0002-1527-4376

Abstract

The numerous drawbacks of the lock and key security system, have necessitated the development of automated door lock systems. In this paper, a hybridized security door with password-based access and SMS notification enhancement was designed to ensure house owners security and eliminate the cost of replacement of key when misplaced. The system comprises of a Passive Infra-Red (PIR) motion sensor module that detects movements of any object around its front surface coupled with the GPRS module, PIC16F877A Microcontroller unit (MCU) and other electronic accessories. Once motion is detected by the PIR, the system activates the MCU to initiate the lock and unlock process via the inputting of a password. The MCU also activates the GSM module to send an SMS to the house occupant when the system notices an unauthorised user. The system categorises a person as an unauthorised user when a wrong password is entered three times. The developed system was able to give a correct visual report of "access denied" to any unauthorized user and as well as send a timely SMS alert to the occupant via a registered mobile number for unusual password access denial notification.

Keywords: GSM module, microcontroller, password-based-locks, security, SMS notification

INTRODUCTION

The conventional security system employed in most homes and offices in Nigeria usually employs the use of lock and keys which must be carried by the occupant. This system was identified to have some drawbacks which make it less effective for protection. Some of the identified drawbacks are as follows: the burden of carrying bunches of the key around; loss or misplacement of a key might require destruction of the lock and/or replacement with the new one, which may apart from the cost of purchasing a new lock and replacement, require that the whole door is pulled down to remove and replace the lock.; an occupant cannot access his/her lock from a remote site; an attempt by an intruder may not be noticed until after the damage is done; and a key may also be stamped easily on semi-solid objects like soap by a burglar to make copies of it later (Divya & Mathew, 2017, Wei, 2020).

It is crucial to develop an improved lock security system that is not encumbered by the aforementioned problems and yet enhances the security of life and properties. Efforts have been directed toward developing electronic door lock systems. Various digital-electronic door locking systems have been reported in the literature. They include: "electronic locking system operated by the combination of a digital key, security password or number codes" (Hwang & Baek, 2007), Radio Frequency Identification (RFID) based locks (Verma & Tripathi, 2010, Park et al., 2009), "design of both a Near Field Communication (NFC) and a smartphone to achieve a door lock control system" (Hung et al., 2015), smart door lock system based on blockchain (Han et al., 2017) and Internet of Thing (IoT) enabled door lock system (Adiono et al., 2019, Jeong, 2016).

Other door lock units have been based on one biometric feature or the other. Examples are the face recognition based lock proposed by Hassan et al. (2012) and Lim et al. (2013), fingerprint-based ones proposed by Ping et al. (2010) and Kader et al. (2016), and palmtop recognition based system proposed by Nafi et al. (2012). Some researchers have even developed a hybrid digital lock system which combines two or more technologies. A quick example of this is the work of Adalan & Erkmen (2016) who proposed a face recognition, NFC and voice-controlled door lock unit. Komol et al. (2018) based their lock system on RFID and fingerprints.

Amanullah (2013) utilised a matrix keypad as depicted in Figure 1. An individual is required to enter the code in the matrix keypad, which is then confirmed by the microcontroller for opening or otherwise. However, when a wrong code is entered a red signal will be displayed. Global System for Mobile Communication (GSM) or Code Division Multiple Access (CDMA) module may be employed to operate the device when a person requesting access initiates a call from his mobile device the receiving

device accepts the call and if it from a stored number, the door unlock process will be initiated and the door will open. An Integrated Power System (IPS) circuit was recommended for providing backup in case of emergency when there is a failure in supply.

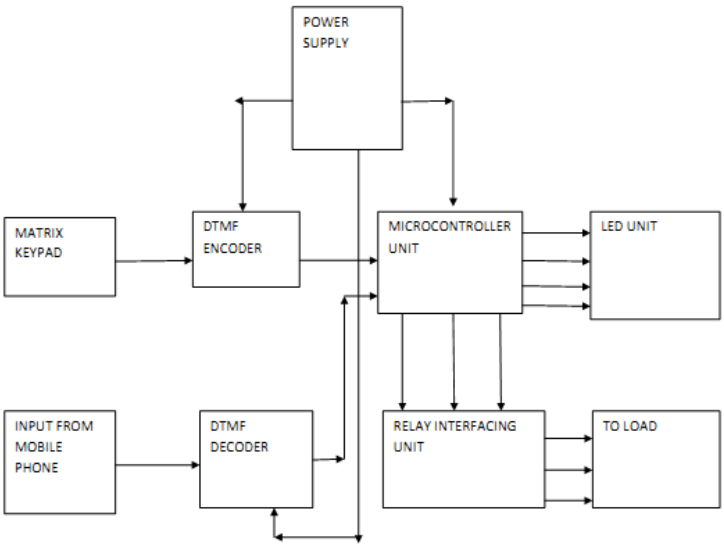


Figure 1: Block diagram of the door lock system with matrix keypad (Amanullah, 2013)

In Ha (2015), an electronic door lock system, which operates with the Internet of Things (IoT) was developed. It was designed and implemented to enhance security and convenience. The system can acquire the image of the unauthorised (invalid) user and send the same to a mobile device. It sends an alarm notification to "the mobile device when the door lock is physically damaged". The flow chart of the proposed system is shown in Figure 2. However, the fact that this requires image file transfer, which could be a challenge in an environment with poor internet connectivity is a drawback to this system.

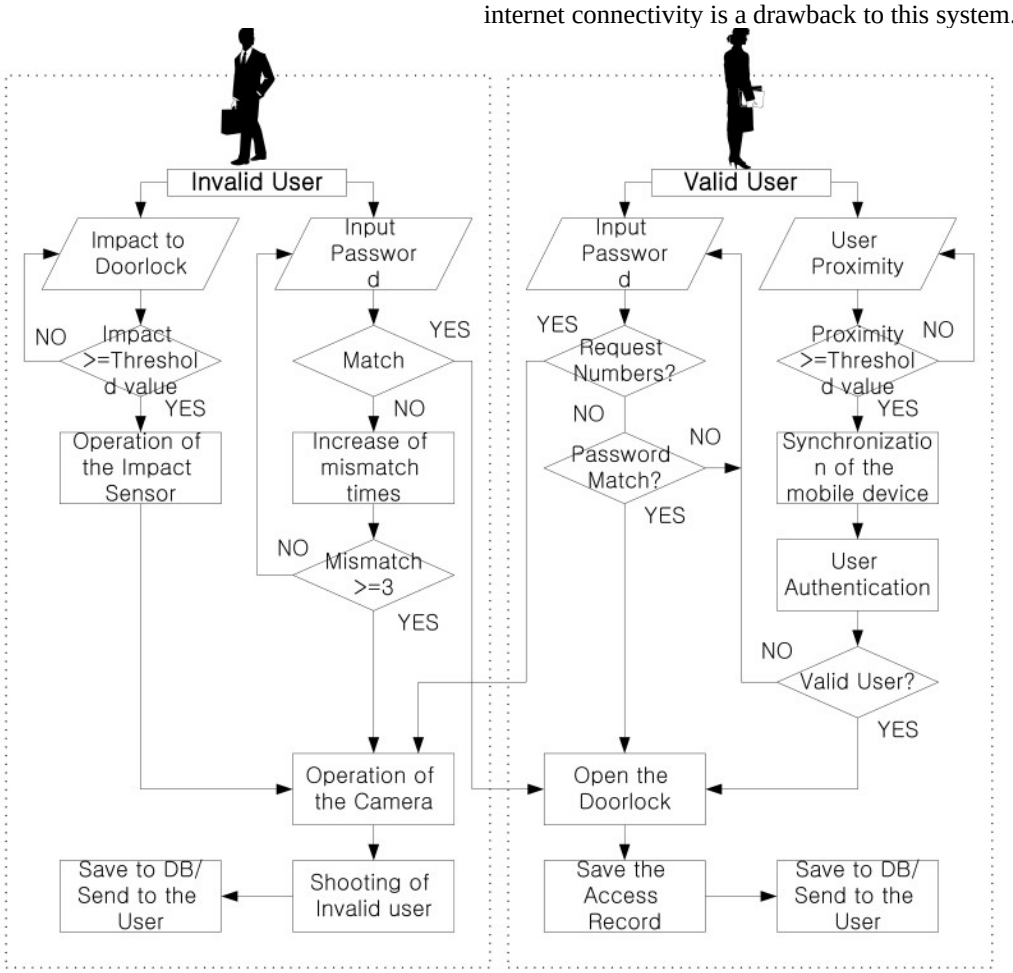


Figure 2: Digital Door Lock Procedures for Invalid and Valid Users (Ha, 2015)

Ibrahim et al. (2015) proposed the design of a GSM-based digital door lock security system using the PIC platform. A user is required to provide a 5-digit password to lock or unlock the motorised. When three consecutive wrong password attempts are observed, a warning message will be sent to saved mobile numbers for appropriate action. The block diagram is shown in Figure 3.

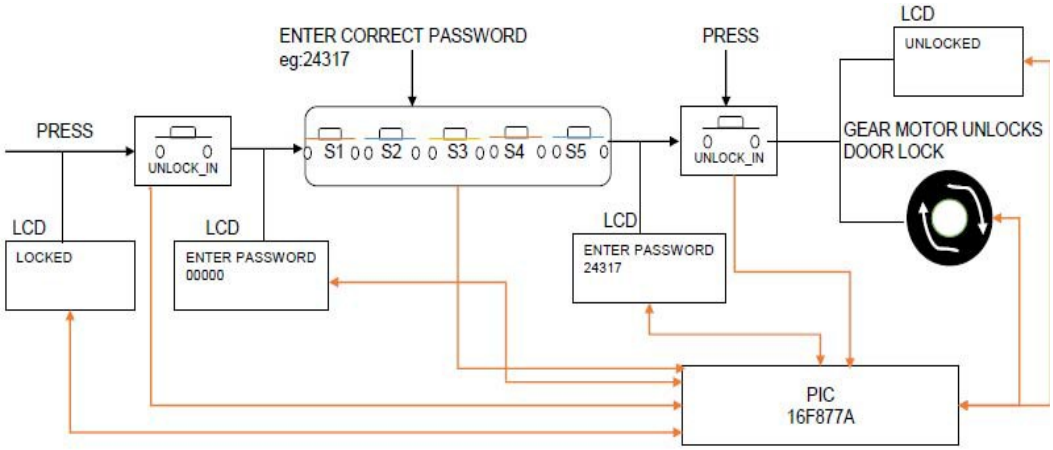


Figure 3: Unlocking stage of the door lock system (Ibrahim et al., 2015)

Hence, in this study, a password-controlled security door with SMS based notification systems was developed with an emphasis on prevention of burglar attack. This is achieved by implementing it with a system that supplements human ability to sense, monitor, display, observe, calculate and control. This work seeks to add to the existing set of works focusing on the password-controlled door lock system such as those of Amanullah (2013), Ha (2015), Ibrahim et al. (2015). In addition to being password-based, an SMS notification system was included to alert the occupant of the house with the locked

The interconnection of the proposed password-controlled security door system with Short Message Service (SMS) for notification is shown in Figure 4. The door lock unit has an embedded motor unit (not shown). Its opening and closing are controlled by the relay switch based on the sensed signal from the motion sensor (for intrusion detection) and keypad entries. The display unit indicates whether or not access is granted or denied.

door in the event of an intrusion by an unauthorised person(s). Given unreliable network connectivity, an intruder image acquisition feature was not integrated.

The password-based security door system was favoured in this work over the biometric-based types since the former allows for multiple users. Thus, the password-based security door system is more suitable for the office environment and family settings where more than one person usually require access.

MATERIALS AND METHOD

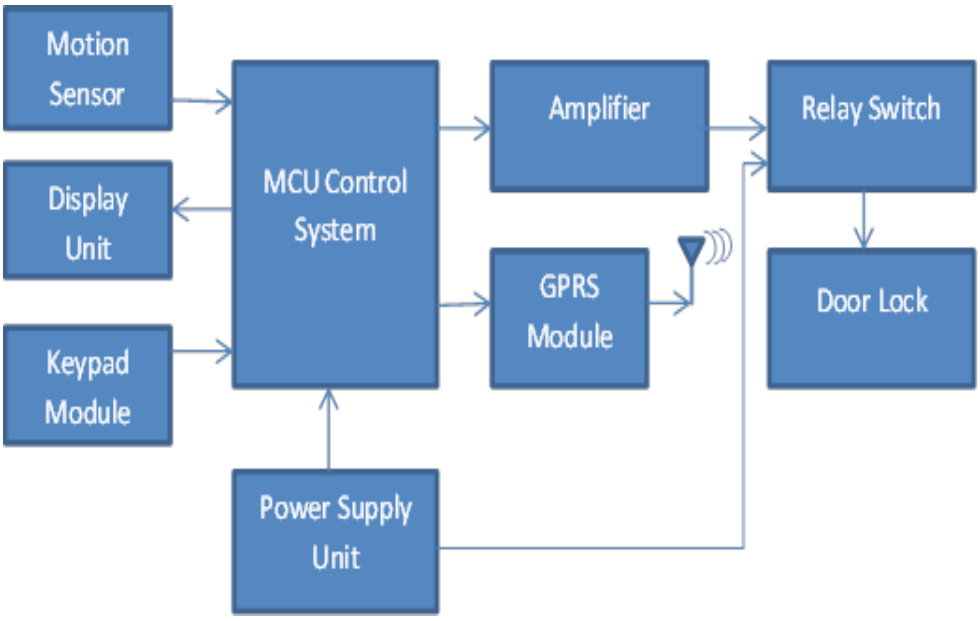


Figure 4: Block diagram of the proposed system

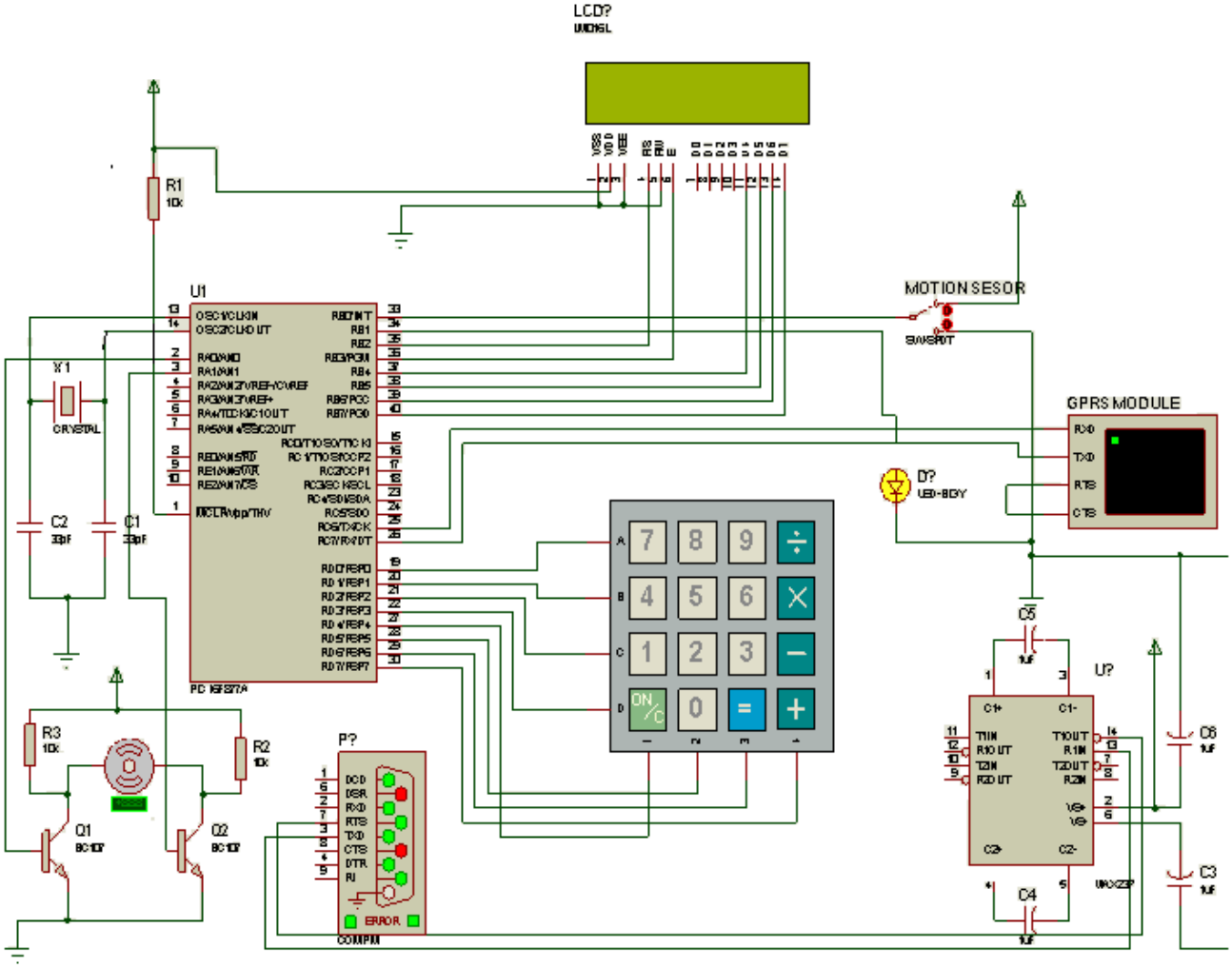


Figure 5: Design and Construction of Password Controlled Security Door System with SMS Alert

Figure 5 depicts the circuit diagram for the Password Controlled Security Door System with SMS Alert. It comprises of the Power Supply Unit, Relay Circuit, Control Circuit, 4 × 4 matrix keypad, DC motor and Display Unit. It also included a Passive Infra-Red (PIR) motion sensor module that detects movements of any object around its front surface. The PIR was coupled with a GPRS module, PIC16F877 Microcontroller and other electronic accessories such as quartz crystal, ceramic capacitors, polarised capacitors, resistors, and son.

PIC 16F877A is a 40-pin 8-Bit CMOS FLASH microcontroller from Microchip as shown in Figure 6. Since it follows the Reduced Instruction Set Computer (RISC) architecture, all single cycle instructions take only one instruction cycle except for program branches which take two cycles (Ibrahim et al., 2015).

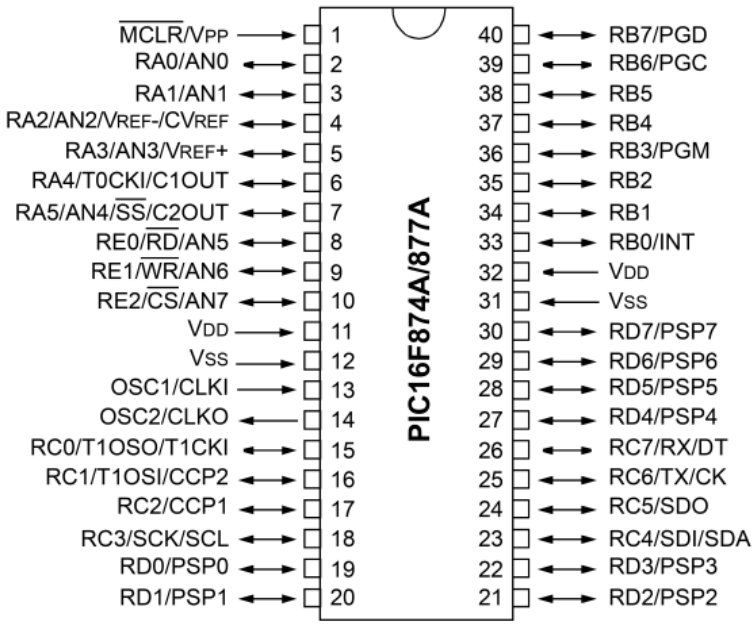


Figure 6: PIC16F877 pin configuration (Microchip, 2003)

PIC16F877 comes with three operating speeds with 4, 8, or 20 MHz clock input. In this case, 8 MHz quartz crystal oscillator (X1) for the same which was fed through the OSC1 and OSC2 ports of PIC. The ports 11 and 32 were shorted. The ports 12 and 31 were grounded. The controller used a +5v source obtained via a regulated DC voltage obtained from a regulator. A 9v DC battery power source is used. But to guarantee a smooth operation two ceramic capacitors C1 (33 pF) and C2 (33 pF) were used.

PIC16F877 was interfaced with the GSM module via TX port of PIC16F87 (port number 25) and RX port of GSM. The GSM module is for sending SMS when an unauthorised user is observed. The GSM module is as shown in Figure 7.

Figure 7: Commercially available GSM module

The system can provide feedback to users via an LCD screen. In this case, the JHD162A 16 x 2 LCD was used. The JHD162A 16 x 2 LCD has 16 pins and can be operated in 4-bit mode or 8-bit mode (Alldatasheet.com). In this research, the LCD module was operated in the 4-bit mode. The name and functions of each pin of the JHD162A LCD module are as explained in Table 1.

Table 1: JHD162A 16 x 2 LCD Pin description

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VSS	VCC	VEE	RS	R/W	E	DB0	DB1	DB2	DB3	DB4	DB5	DB6	DB7	LED+	LED-

The pins 11,12,13,14 of LCD module are interfaced through ports 35,36,37,38 respectively of PIC. The pins 4, 6 of LCD module are interfaced through ports 33, 34 respectively of PIC. The pins 1, 5 of LCD module are shorted and grounded and pin 2 is supplied with +5V. Other details of the JHD162A 16 x 2 LCD may be seen in (Alldatasheet.com).

To enter the password, a 4x4 keypad matrix with 8 pins divided into 4 rows and 4 columns was used. When a button is pressed, one-row pin will be shorted out with a column pin. For example, if you press button "1", row "0" will be connected to column "0" (Pelayo, 2020). The circuit structure of the 4x4 Matrix keypad is shown in Figure 8.

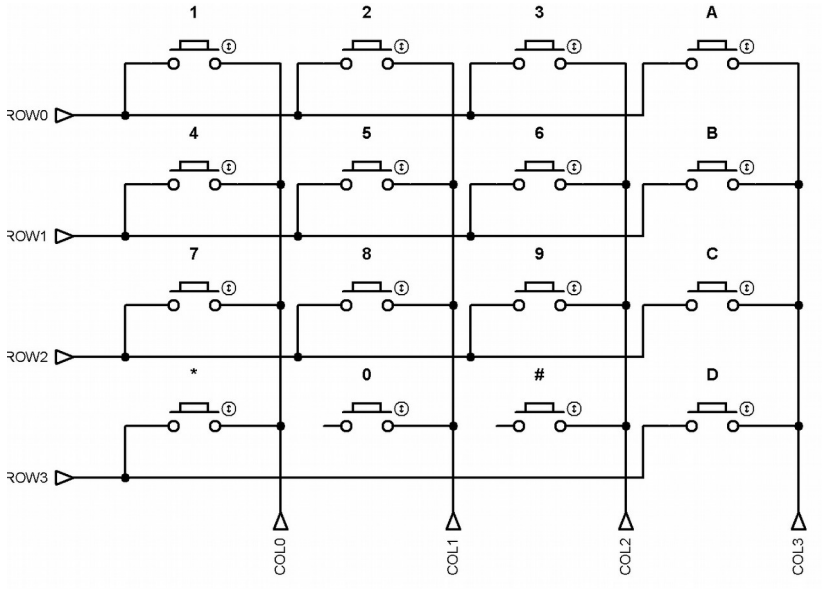


Figure 8: Circuit structure of the 4 X 4 Matrix keypad

A programme instruction must be loaded into the microcontroller unit (MCU) via Keil µVision IDE and Willar Programmer for decision making

2.1. Programme Algorithm

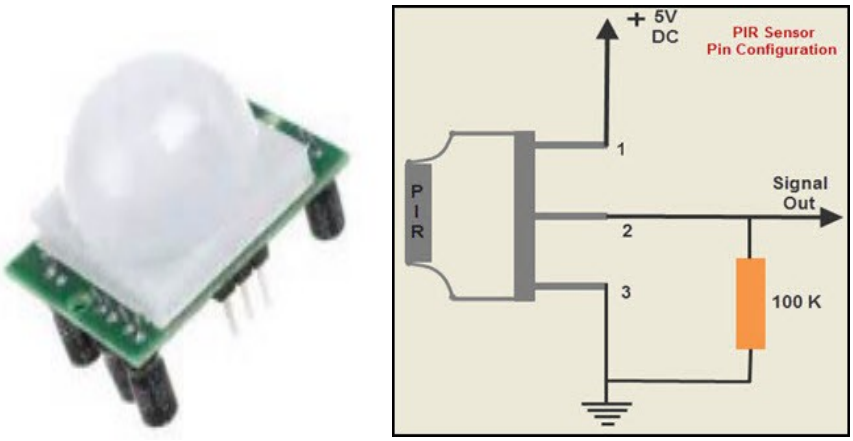
The Proteus software wax used for the circuit diagram and simulation. The procedure followed by the MCU in deciding whether to initiate the door unlocking process is outlined below.

STEP1: Start;
STEP2: Input MD = motion detector state;
STEP3: IF MD == false THEN;
STEP4: SLEEP 20 sec;
STEP5: GOTO STEP2:
STEP6: END IF
STEP7: ATEMPT=1
STEP8: DISPLAY ‘ENTER PASSWORD’
STEP9: KP=GET 4 KEYPAD KEY PRESSED
STEP10: PW=GET EEPROM PASSWORD
STEP11: IF KP != PW THEN
STEP12: IF ATEMPT>4 THEN
STEP13: SEND SMS ALERT
STEP14: WAIT 15MIN
STEP15: GOTO STEP18;
STEP16: END IF [STEP12]
STEP17: ATEMP=ATEMP +1;
STEP18: DISPLAY ‘PASSWORD ERROR‘

STEP19: GOTO STEP8;
STEP20: END IF [STEP11]
STEP21: OPEN DOOR;

STEP22: WHILE(MOTION DETECTED) WAIT 20 SEC
STEP23: CLOSE DOOR;
STEP24: GOTO STEP2

The passive infrared (PIR) motion sensor shown in Figure 9 is required to detect when someone approaches the door. This is required to reduce the power consumption of the device by putting the device to sleep when nobody is accessing the door. However, the system automatically wakes when movement near the door is detected by the PIR sensor.



(a) (b)

Figure 9: PIR Motion Sensor (a) and its Pin Configuration (b)

SYSTEM TESTING AND IMPLEMENTATION

3.1. Breadboard Testing and Construction

This project work was first arranged and tested on a breadboard before transferring it to the Vero board for final soldering and implementation as depicted in Plate 1. The constructed system was tested stage by stage to ascertain that the circuit operation conforms to the model design for this project and meets expectation.

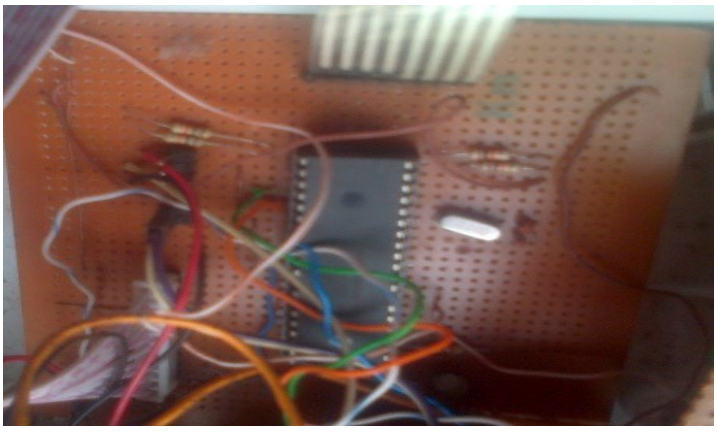


Plate 1: Soldered Components on the Vero board

The completed project work was placed in a thermoplastic casing as shown in Plate 2. The keypad was placed just below the screen for easy accessibility, this is to allow the user not to obstruct his/her view while pressing the keypad and observing the entry on the screen of the LCD Display. The antenna showing at the top of the package was connected to the GSM Module used. This was positioned in such a way to allow good signal strength to be trapped by the GSM Module.

Plate 2: Completed project construction

3.2. Testing

When the completed construction was powered, the LCD screen is OFF; this was done to save energy consumed by the system. Likewise, the MCU by default goes to sleep mode when powered and not in use.

Once motion is sensed by a motion sensor attached to PORTB0, the MCU waked up automatically and requests for password input from the user as shown in Plate 3. Upon successful entry of a correct password, "Access granted" was the display and the door lock was unlocked. However, when a wrong password is entered, "Access Denied" is indicated as shown in Plate 4.

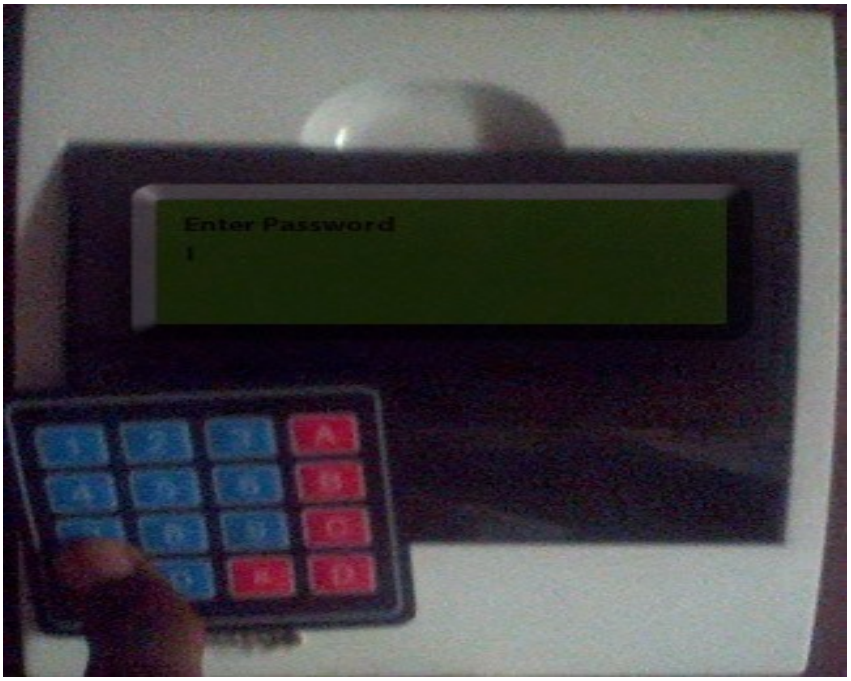


Plate 3: Password entry screen

In the last phase of the test, the construction was mounted on a small portable board serving as a door prototype for easy mobility as shown in Plate 5. The door prototype was closed and the wrong password was deliberately attempted three consecutive times. For each wrong attempt "Invalid password" was displayed as shown in Plate 4. No further password input was allowed for a preset time duration of 10 minutes after the third wrong password attempt. Then an SMS alert was sent to a phone number coded with the device. This phone number belongs to the house occupants. This 10 minutes' delay was assumed to be long enough for the occupant to contact people around for a check on the door and to effect proper action such as arrest if need be.

Plate 4: Invalid Password and Access Denied

Plate 5: The System mounted on Portable Cupboard

CONCLUSION AND RECOMMENDATION

4.1. Conclusion

This report presented information for the development of a hybridized security door with password-based access and SMS notification enhancement. This will ensure house owners security and eliminate the cost of key replacement when they are misplaced. The system consisted of hardware components such as the MCU, LCD, PIR and other electronic components. The MCU was programmed to make the lock and unlock decision.

The use of password and LCD screen made the system interactive and user-friendly.

To ensure system simplicity, a minimum number of electronics components was used to accomplish the desired result and at the lowest possible cost while maintaining the quality, performance and functionality of the system.

4.2. Recommendation

Future work can make the SIM number of the house occupant preloaded in the program code editable in case the user lost the SIM card. The system will be more robust if a biometric feature is used in combination with this password-controlled door lock system. This will provide two-factor authentication for enhanced security. Apart from using a PIR-based motion sensor for intrusion detection, other methods can be investigated given the limitations of PIR. Moreover, owing to the possibility of wireless network failure, two SIMs belonging to different networks can be introduced. These SIMs should be coded with two priorities. The first SIM should be assigned a higher priority and the second SIM, assigned a lower priority. The system should be configured in such a way that when the SIM with the highest priority fails to send an SMS message or there is no read receipt, then the SIM with the lower priority should proceed after a set interval. It is expected that this should improve wireless network reliability.

Finally, to minimize disruption to an already mounted door in a house and its consequential increased cost, it is recommended that door manufacturers be carried along in the physical realisation of this research so that they can build in this hybridized security door with password-based access and SMS notification enhancement right from the door making process. So when a new door is to be mounted on a house, it will have included the developed system.

REFERENCES

Adalan, K., & Erkmen, B. (2016). Face recognition, NFC and voice-controlled door lock system. In *2016 National Conference on Electrical, Electronics and Biomedical Engineering (ELECO)* (pp. 696-700). IEEE, Bursa, Turkey.

Adiono, T., Fuada, S., Anindya, S. F., Purwanda, I. G., & Fathany, M. Y. (2019). IoT-Enabled door lock system. *International Journal of Advanced Computer Science and Applications*, *10*(5), 445-449.

Alldatasheet.com. JHD162A Series. https://pdf1.alldatasheet.com/datasheet-pdf/view/127934/ETC1/JHD162A.html. Retrieved 12/15/2020.

Amanullah, M. (2013). Microcontroller based reprogrammable digital door lock security system by using keypad & GSM/CDMA technology. *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, *4*(6), 38-42.

Circuit Today. (2020). How to Interface GSM Module to 8051 Micro Controller-Send and Receive SMS. Available: https://www.circuitstoday.com/interfacing-gsm-module-to-8051. Retrieved 12/15/2020.

Divya, R. S., & Mathew, M. (2017). Survey on various door lock access control mechanisms. In *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)* (pp. 1-3). IEEE.

Ehiagwina, F. O., & Olaiya, O. O. Development of a password-controlled security door with short messaging service based notification system. *5th International Conference and Exhibition of School of Science (Virtual).* School of Science, Yaba College of Technology, Lagos State, Nigeria.

Ha, I. (2015). Security and usability improvement on a digital door lock system based on internet of things. *International journal of security and its applications*, *9*(8), 45-54.

Han, D., Kim, H., & Jang, J. (2017). Blockchain-based smart door lock system. In *2017 International conference on information and communication technology convergence (ICTC)* (pp. 1165-1167). IEEE, Jeju Island, Korea.

Hassan, H., Bakar, R. A., & Mokhtar, A. T. F. (2012). Face recognition based on auto-switching magnetic door lock system using

microcontroller. In *2012 International Conference on System Engineering and Technology (ICSET)* (pp. 1-6). IEEE, Bandung, Indonesia.

Hung, C. H., Bai, Y. W., & Ren, J. H. (2015, June). Design and implementation of a door lock control based on a near field communication of a smartphone. In *2015 IEEE International Conference on Consumer Electronics-Taiwan* (pp. 45-46). IEEE, Taipei, Taiwan.

Hwang, I. K., & Baek, J. W. (2007). Wireless access monitoring and control system based on digital door lock. *IEEE Transactions on Consumer Electronics*, *53*(4), 1724-1730.

Ibrahim, A., Paravath, A., Aswin, P. K., Iqbal, S. M., & Abdulla, S. U. (2015). GSM based digital door lock security system. In *2015 International Conference on Power, Instrumentation, Control and Computing (PICC)* (pp. 1-6). IEEE, Thrissur, India.

Jeong, J. I. (2016). A study on the IoT based smart door lock system. In *Information Science and Applications (ICISA) 2016* (pp. 1307-1318). Springer, Singapore.

Kader, M. A., Haider, M. Y., Karim, M. R., Islam, M. S., & Uddin, M. M. (2016). Design and implementation of a digital calling bell with door lock security system using fingerprint. In *2016 International Conference on Innovations in Science, Engineering and Technology (ICISET)* (pp. 1-5). IEEE, Chittagong, Bangladesh.

Komol, M. M. R., Podder, A. K., Ali, M. N., & Ansary, S. M. (2018). RFID and Finger Print Based Dual Security System: A robust secured control to access through door lock operation. *American Journal of Embedded Systems and Applications*, *6*(1), 15-22.

Lim, J., Kim, C., Cha, W., Han, T., Huh, G., Song, S., & Lee, S. (2013). Reliable digital door lock control system using face recognition. *Journal of Institute of Korean Electrical and Electronics Engineers*, *17*(4), 499-504.

Microchip. (2003). PIC16F87XA Data Sheet: 28/40/44-Pin Enhanced Flash Microcontrollers

Nafi, K. W., Kar, T. S., & Hoque, S. A. (2012). An advanced door lock security system using palmtop recognition system. *International Journal of Computer Applications*, *56*(17), 18-26.

Park, Y. T., Sthapit, P., & Pyun, J. Y. (2009). Smart digital door lock for the home automation. In 2009 *TENCON-IEEE Region 10 Conference* (pp. 1-6). IEEE, Singapore.

Pelayo, R. (2020). Arduino keypad: interfacing with 4x4 matrix. https://www.teachmemicro.com/arduino-keypad-interfacing-4x4-matrix. Retrieved 15/12/2020.

Ping, W., Guichu, W., Wenbin, X., Jianguo, L., & Peng, L. (2010, May). Remote monitoring intelligent system based on fingerprint door lock. In *2010 International Conference on Intelligent Computation Technology and Automation*, *2*, 1012-1014). IEEE, Changsha, China.

Verma, G. K., & Tripathi, P. (2010). A digital security system with door lock system using RFID technology. *International Journal of Computer Applications*, *5*(11), 6-8.

Wei, S. (2020). Research and Application of Smart Lock Safety Management and Control System. In *Journal of Physics: Conference Series* (Vol. 1601, No. 5, p. 052038). IOP Publishing.