SCIFED Publishers

Ajao LA, SF J Telecommunic, 2018, 2:2

SciFed Journal of Telecommunication

Research Article Open Access

A Smart Door Security-Based Home Automation System: An Internet of Things

*[1]Ajao LA, [2]Kolo JG, [3]Adedokun EA, [4]Olaniyi OM, [5]Inalegwu OC, [6]Abolade SK

*[1,2,4,5]Department of Computer Engineering, School of Electrical Engineering and Technology, Federal University of Technology, Minna, Nigeria

[3]Department of Computer Engineering, Faculty of Engineering, Ahamadu Bello University, Zaria, Nigeria

Abstract

The recent advancement in smart technology design with integration of smart sensors and embedded components has rapidly improved human lives in so many areas which includes home automation, smart phones, smart healthcare, smart cars and so on. Therefore, smart home security demand serious attention and is indispensable in this era of internet of things communication over 6LowPAN model using IPv6 addresses for interconnectivities and end-to end links. In this paper, the access control, embedded sensors and alarm systems are used for safeguard the device facilities in the home automation for authentication or authorization and users management over the network. However, wireless technology (such as GSM, ultrasonic sensor, and Bluetooth low-power enable) was used for controlling and monitoring home entrance, user authentication, authorization and smart devices management. An android web application was also developed and integrate with the system for home user control remotely. This developed system was equipped with a strict access control and password security features for an intruder denial or violation and also keep the neighbor's alert of possible human attacks.

Keywords

Authorization; Human Attack; Smart Technology; Sensors; Security; 6lowpan

Introduction

The advent of intelligence home appliances based embedded sensors and wireless technology has improved the home livings with several domestic appliances which includes washing machines, cloth dryers, refrigerators, electric and gas cooking materials, dishwashers, sewing machines, television and home theater gadget [1, 2]. Therefore, security of life and property is a key responsibility of every citizen in a country where these social infrastructures based internet of things appliances are been implemented.

Security is described as countermeasure that resist or protection against any harmful attacker which are widely applicable to any vulnerable host or valuable asset in a network such as smart appliances, user data, and many others. One of the fastest emergent technologies in the universal network is home automation system which contains various domestic appliances for the user enjoyment and comfortability. The smart devices require adequate security for user data controlling, monitoring, management, and securing every device itself. Home automation is define by [3] as home-owner that contains many intelligence domestic appliances for users living comfortability and ease of achieving many system operations and control remotely. Home security is the most visible element in home computerization.

***Corresponding author:** Ajao LA, Department of Computer Engineering, School of Electrical Engineering and Technology, Federal University of Technology, Minna, Nigeria. E-mail: ajao.wale@futminna.edu.ng

Received May 17, 2018; **Accepted** July 2, 2018; **Published** July 13, 2018

Citation: Ajao LA (2018) A Smart Door Security-Based Home Automation System: An Internet of Things. SF J Telecommunic 2:2.

A conventional method of securing home has improved significantly compared to the past decades. Today, embedded sensor, digital camera, GPS/GPRS and many others have been discovered for the efficient implementation of home automation security monitoring, intruder detection and managing of smart home technology facilities [4, 5].

The smart embedded wireless sensors devices has gain more attention in the era of Internet of Things technology for surveillance, tracking, monitoring and remote smart home control and applications [6]. This is as a result of widely applications in the electronics industries, automobiles, robotics, military for security, surveillance and so on. The importance of smart embedded sensors claims in the smart technology particularly smart home environment has raises some threat of cyber-attacks, hackers, wormhole attacks, services availability (such as flooding, spoofing, jamming, and replay attacks), unauthorized routing update, unauthorized node access (such as impersonation or eavesdropping attacks).

The first remote home automation control technology was developed with X10 network technology for signaling transmission and communication between electronics home devices. This smart home technology was classified into three generation categories which are home automation wireless technology with proxy server using ZigBee, Bluetooth, Wi-Fi, and so on. These wireless technology approaches are discussed in [2, 3, 7, 8], others are artificial intelligence control and computational intelligence based robotic system or embedded system with human interaction (Rooma and Rovio robot) [9]. Also, implementation of central gateway or user interfaces such as wall terminals, computer system, mobile phone apps or android web apps through the universal network [10, 11] which can be achieved through smart technology security.

Smart embedded wireless sensors devices have gain more attention in the era of Internet of Things technology for surveillance, tracking, monitoring and remote smart home control and applications [12]. This is as a result of the wide applications in the electronics industries, automobiles, robotics, military tracking and investigation.

2. Related Works

The HAS is vulnerable to different threats or attacks since most of their devices depend on the universal networks. These attacks are physical attack, nefarious attack, eavesdropping, interception, hijacking and spoofing and many others[13, 14].Also, the proliferation of smart embedded sensors particularly in smart home environment has raised some threat of cyber-attacks, hackers, wormhole attacks, services availability (such as flooding, spoofing, jamming, and replay attacks), unauthorized routing update, unauthorized node access (such as impersonation or eavesdropping attacks). Therefore, the need for a robust security is significant to study.

The first remote home automation control technology was developed with X10 network technology for signaling, transmission and communication between electronics home devices. Smart home systems have tremendously developed over the years, adopting various technologies: ZigBee [2], Bluetooth [15], RFID [9], GPRS/GSM [2, 4, 10, 14], and so on. The 2010 report by the Alarm Industry Research and Educational Foundation [15] states that burglars spends fewer than 60 seconds to break into a home [AIREF]. Deductively, any measure established that makes a facility more difficult to access, will inherently serve as a deterrent [7]. Some structures have employed artificial intelligence (AI) control and computational intelligent based robotic systems with human interaction [16]. Also, implementations of central gateway or user interfaces such as wall terminals, computer system, mobile phone apps or android web apps through the universal network were presented in [10, 11].

The HAS is vulnerable to different threats or attacks since most of their devices depend on the universal networks. These attacks are physical attack, nefarious attack, eavesdropping, interception, hijacking and spoofing and many others [17]. The authors in [18] also demonstrated the possibility of a real-time remote monitoring via an IoT based doorbell. All of these are evident of the limitless applications for IoT based smart security systems. Since security systems have often been breached by intelligent thieves, it becomes so necessary for the deterring measures in place to also advance ahead of the criminals.

3. Methods and Materials

The embedded smart sensor approach integrated with other wireless components was employed in the door security based home automation monitoring. The system coding and development for an IoT-based smart home door security involves integration of both hardware and software system design. The embedded software coding was implemented in Arduino integrated development

environment (IDE) using C language. The wireless based home appliances are control remotely with the development of an android application using eclipse IDE.

This system is flexible and friendly to operate. When the system is power ON, it will initialized all the modules connected to it which includes servo motor, keypad, LCD display, buzzer, Bluetooth module, and GSM module. The door security home automation systems allow the user to enter password for door opening or closing. The password will be verified for its validity or denial before further action is taken. If the password is valid, the door will open and if wrong password is enter after four attempts, the system is programmed to report unauthorized user which signal the controller to send alert to buzzer and GSM module for buzzing and sent message as illustrated in the flowchart of Figure 1. Figure 2 shows the smart door security based IoT block diagram. (Figures 1, 2)

Figure 1: Home Automation Door Security System Based Iot

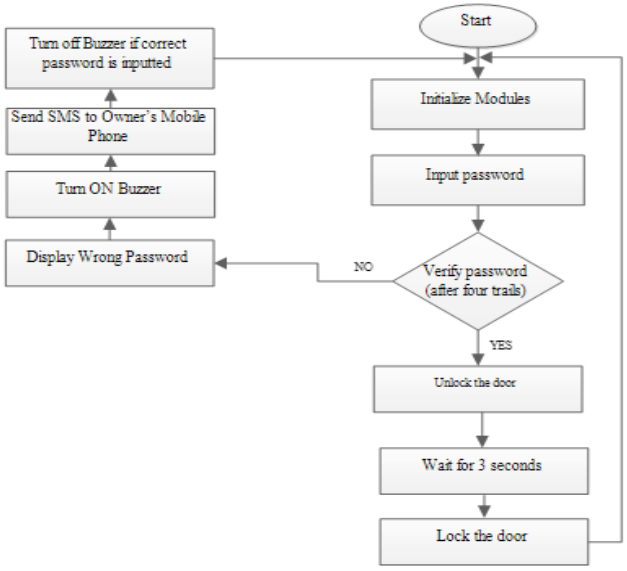
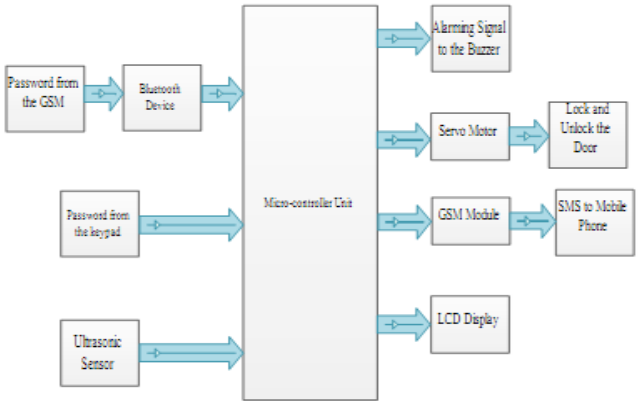


Figure 2: Home Automation Door Security System Block Diagram



3.1 Hardware Module

3.1.1 Controller Unit

The integration of hardware system for home automation door security consists of Arduino Uno integrated with Atmega 328 for system processing and servo motor used for control of opening and closing of the home automation door. The Arduino Uno external architecture and its features are illustrated in (Figure 3).

Figure 3: Arduino Uno (Atmega 328) External Architecture

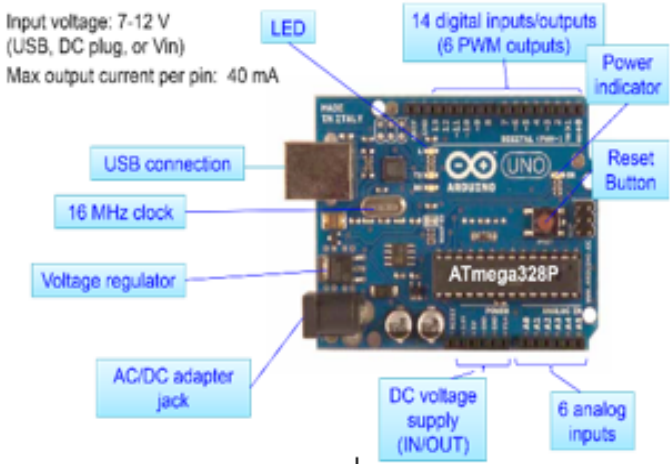


Figure 4A: Internal Architecture of Servo Motor

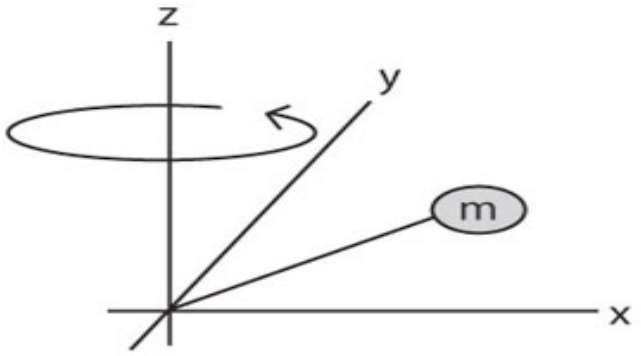
Figure 4B: External Architecture SM

3.1.2 Servo Motor

The drive security door mechanism is servo motor which helps in control of the door opened and closed, the mechanism dimensions, mass and friction coefficient are calculated for load determination. This device can be described as an actuator or closed loop system that

produces a rotary motion or toque, enable the precise movement of angular velocity, acceleration and linear position with suitable embedded sensor integrated with motor for feedback position. Servo motor consist of both input signal (analogue or digital) which signifying the output shaft position as commanded by the controller. This servo mechanism consists of three pin connection PWR, GND and DATA. It has 4.0kgcm torque, Size (L * W * H): 20.0 * 17.6 * 8.0mm, operation voltage 4.8 ~ 6.0V, Speed 0.12sec/60°without load and operating current of 100mA [20]. The internal and external architecture are illustrated in Figure 4a and 4b respectively. (Figures 4a, 4b)

Figure 5: Servo Mechanism Rotational of Inertial Moment



The inertial moment (J) in (oz-in-sec²**),** rotation of servo motor, speed and load torque as shown in (Figure 5), can be calculated as expressed in Equation 1, to 4 reverentially.

$$J = \iiint \rho(\chi^2 + y^2)\, d\chi\, dydz \quad (1)$$

$$J = mL^2 \quad (2)$$

$$S = \frac{D}{T} \quad (3)$$

$$S_m = \frac{D}{(T - A_t)} \quad (4)$$

where, m is mass, L is distance between center of gravity and rotational center, S_m is servo motor speed (m/s), T is time (s), and A_t is acceleration time in (m/s²).

For the safety factor, the torque required can be calculated by multiplying the sum of load torque with acceleration torque as given in Equation 5, and the effective load torque for fast cycle operation pattern can be calculated where acceleration divided by deceleration is frequent as expressed in Equation 6.

$$T_M = (T_L + T_a) * S_f \quad (5)$$

$$T_{rms} = \sqrt{(T_a + T_a)^2 * t_1 + TL^2 * t_2 + (T_d + T_L)^2 * t_3 / t_f} \quad (6)$$

Where, T_M is torque required, T_L is load torque, T_a is acceleration torque and S_f is safety factor.

3.1.3 Output Unit

The buzzer implemented for blow alarm in case of any intruder detection. The liquid crystal display unit was used for HA door security message display, it consists of 16 pins connection as illustrated in Figure 4a and 4b. The pin 1, 2 and 3 are Ground (VSS), 5V power (VDD) and contrast voltage (VE) respectively. The Pin 4 is the register select (RS), and when this pin is LOW, data transferred to the display is treated as commands. When RS is HIGH, character data can be transferred to and from the module. Pin 5 is the read/write (R/W) line. This pin is pulled LOW in order to write commands or character data to the LCD module. When this pin is HIGH, character data or status information can be read from the module. Pin 6 is the enable (E) pin, which is used to initiate the transfer of commands or data between the module and the microcontroller. When writing to the display, data is transferred only on the HIGH-to-LOW transition of this line. When reading from the display, data becomes available after the LOW-to-HIGH transition of the enable pin, and this data remains valid as long as the enable pin is at logic HIGH. Pins 7 to 14 are the eight data bus lines (D0 to D7). Data can be transferred between the microcontroller and the LCD module using either a single 8-bit byte or as two 4-bit nibbles. In the latter case, only the upper four data lines (D4 to D7) are used. The 4-bit mode means that four fewer I/O lines are used to communicate with the LCD. (Figures 6a, 6b) illustrate LCD architecture.

Figure 6A: LCD Back-View Architecture

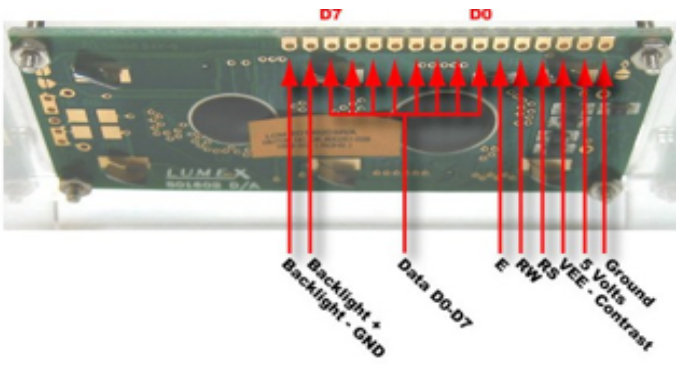


Figure 6B: LCD Front-View Architecture

3.1.4 The Communication Module

The portable GSM/GPRS module (NEO M590) was employed for remote data communication between the automation home door security and the user android web application. The HC-06 Bluetooth module was used for remote signal control and transmission. This wireless technology based IoT is a serial port profile support chip that allows connection and establishment of serial emulation of microcontroller connection. It enables communication between the devices connected in the universal network using Bluetooth protocol or universal bus (USB) cable.

Bluetooth low power capable of transmitting signal over a range 10 meters maximum and can be configure as a master/slave device, it consume about 30-40 mA current, 3.3 voltage during pairing of devices and 8mA current during communication [21, 22]. The HC-06 Ground (GND) pin is connected to ground, power VCC pin is connected to 5v, transmission/receiver TX/TXD pin is connected to Arduino digital pin 4 and receiver RX/RXD pin is connected to Arduino digital pin 2 as illustrated in (Figure 7), and the Bluetooth communication flowchart is depicted in (Figure 8).

Therefore, the voltage and resistance value used in the system design can be calculated as given in Equation 7.

$$R = V_{cc} - Vf \,/\, If \qquad (7)$$

Figure 7: Breadboard of Bluetooth Circuit Implementation

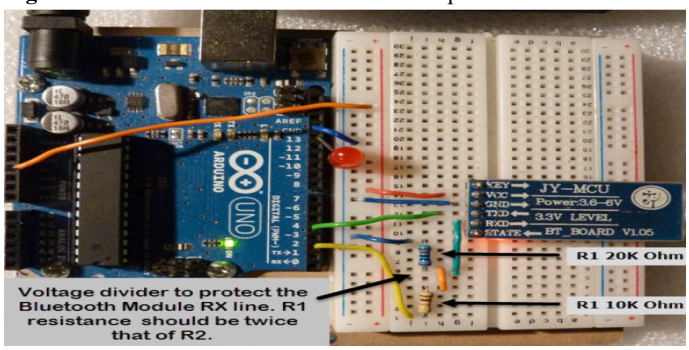
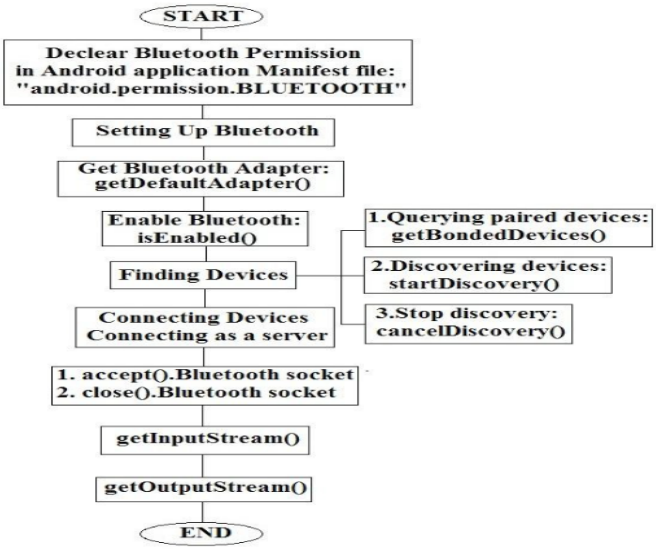


Figure 8: The Flowchart of Bluetooth Communication Process



Where, R is resistor value, Vcc is microcontroller power 5v, Vf is LED voltage reference 0.7v Bluetooth power 3.3v, and current consumption is 30-40mA.

$$R = \frac{5 - 0.7}{4x10^{-3}} = 109.25\Omega$$

$$R = \frac{3.3}{4x10^{-3}} = 82.5\Omega$$

This shows that 100Ω to 110Ω resistor can be used for controller and in the case of Bluetooth implementation required 80Ω to 100Ω for the efficient and reliability of system performance.

Also, the voltage through the Rx/Tx pin of the Arduino can be calculated as in Equation 8.

$$V_{Rx} = Vcc * \frac{R_1}{R_1 + R_2} \qquad (8)$$

$$V_{Rx} = 5 * \frac{20K}{10K + 20K} \approx 3.3\text{V}$$

3.1.5 The Sensing Module

Ultrasonic sensor is integrated into the circuit physical detection or images of any illegal movement detection around the smart home environment. This sensor is electrical transducers that consist of transmitter and receiver, which convert ultrasound waves to electrical signals. It consist of four (4) connected pins, which are ground (GND), power (VCC), trigger (TRIG) and echo (ECHO) pin connection as illustrated in Figure 9. The high voltage of 5v from controller is connected to the TRIG pin to generate high frequency waves within a particular period of time which helps to determine the distance between sensor and the object. (Figure 9)

Figure 9: External Architecture of Ultrasonic Sensor

The distance covered by the ultrasonic sensor can be calculated through the speed of sound produced, the microcontroller takes 11.6ms to received feedback from the sensor, as expressed in Equation 9.

$$D = \frac{speed\ of\ sound \times time\ taken}{2} \qquad (9)$$

Where, speed of sound is given as 344m/s

$$D = \frac{344 \times 11.6 \times 10^{-3}}{2} = 1.9952m \approx 2.0m$$

This shows that each side of ultrasonic sensor can covered a distance of approximately 2 meters apart in detecting object or obstacle in real life application.

3.1.6 Hardwired Program Design

The following lines of code demonstrate the beginning of hardware configuration system based HA door security for the system modules integrations which includes liquid crystal display (LCD), servo motor (SV), 4x4 hexadecimal keypad, ultrasonic sensor and GSM module in Arduino IDE using C-language.

Hardware modules programming

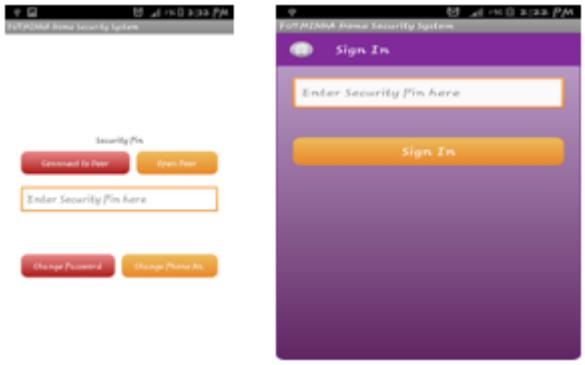
```
#include <Wire.h>
#include <LiquidCrystal.h>
#include <Servo.h>
#include <Keypad.h>
#include <EEPROM.h>
#include <Ultrasonic.h>
Servo myservo;
LiquidCrystallcd(A0, A1, A2, A3, A4, A5);
Ultrasonic ultrasonic(2,3); // (Trig PIN,Echo PIN)

const byte ROWS = 4; //four rows
const byte COLS = 4; //three columns
char keys[ROWS][COLS] = {
{'1','2','3','A'},
{'4','5','6','B'},  //first set of pins are col pins
{'7','8','9','C'},
{'*','0','#','D'}
};

byterowPins[ROWS] = {13, 12, 11, 10}; //connect to the row pinouts of the keypad
bytecolPins[COLS] = {9, 8, 7,6}; //connect to the column pinouts of the keypad

Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS );
String phoneNo="+2348168670476";     //variable to hold phone number
String pin ="1234";
String keyInput ="";
int buzzer =4;
intpinTime=0;
int lock=5;
boolean sent =false;
```

3.2 The software development

The android application platform was developed using java native language with SDK development kit, and it was deployed on the mobile phone for remote door security based HA control, authorization and monitoring. The graphic user interface was developed in the eclipse IDE using XML to link the design to the cloud database system

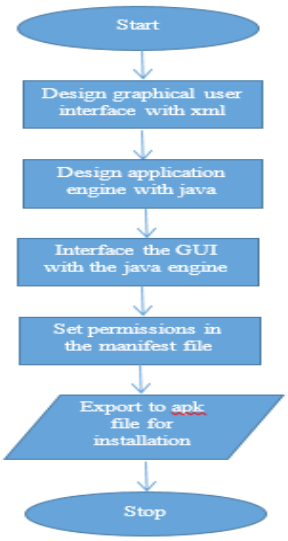
as depicted in Figure 10. The login graphic user interface required a unique home automation user identities like user password and name which denied wrong provisions of user name or password as first level of authorization/ authentication security level. (Figure 10)

Figure 10: Door Security Android GUI



The android application is a mobile operating system that based on the Linux kernel for direct manipulation and mobile operations which includes swiping, tapping, pinching and so on. This apps was developed and powered by Google Incorporation primarily for touch screen mobile operations on the devices like smart phones and tablets. Also, the Eclipse is an integrated development java programming environment that support an android application design for real time purposes and cloud database for data or image storage and retrieval using XML link. This is widely used for programming language like Java, C++, Python, Ruby, and many others. The flowchart illustrated in Figure 11 shows the design flows of an android based Apps. (Figure 11a)

Figure 11A: Android Apps Design Phases



4. Discussions

The smart home automation door security was implemented by integrating the smart embedded sensor system with android mobile apps developed as illustrated in Figure 11a. The embedded sensor security lines of code for door security system based home automation are highlighted. This is strictly design for access control of opening and closing door remotely through wireless communication module (Bluetooth) using a password authentication/authorization techniques. If a valid password is enter through the 4x4 hex keypad implemented at the entrance, this will control the door opening (access granted) and send message to the home user for the security notification. Also, if an invalid password entered, it will denied user access to the entrance of the building (denied access) and send messages for wrong password user trial. This process will allow user trial for four consecutive times before alarm system begin to buzzing for intruder detection. Also, with embedded sensor integration using ultrasonic sensor assist impressively in detection of any movement around the doors or windows in case of burgle and alert the home users with continuous alarm and invader attentive messages sent to the home users as shown in (Figures 11b, 12).

Figure 11b: Door Security Based Smart Home

Figure 12: Security Message Alerts GUI

Door security opening/denial authentication programming

```
lcd.clear();
lcd.print(“ ENTER PASSWORD”);
}
void loop()
{
char key = keypad.getKey();

if(key){
if(key==’A’ || key==’B’ || key==’C’ || key==’D’)
{
if(keyInput.length()>0)
keyInput=keyInput.substring(0,keyInput.length()-1);
}
else {
if(checkForAlarm())
triggerAlarm();
else{
keyInput +=key;
if(keyInput.length()==4){
pinTime++;
if(keyInput==pin)
openDoor();
else
if(pinTime>3)
triggerAlarm();
else
wrongPass();
   }
  }
 }
  String toPrint=””;
for(inti=0;i!=keyInput.length();i++)
toPrint+=’*’;
lcd.clear();
lcd.print(“ ENTER PASSWORD”);
lcd.setCursor(0,1);
lcd.print(toPrint);
}
else
if(checkForAlarm())
triggerAlarm();
}
```

5.0 Conclusion

In this research a smart door security based HAS is developed using smart embedded sensor, wireless communication based IoT and android mobile Apps-based password authorization for adequate security level against intruders. This home automation door security control provides multifaceted levels of user authentication on both hardware system development and android mobile Apps for system resourceful, privacy and trustworthy of the home users or administrator. The door security mobile control system is users friendly and flexible to operate. Based on the detailed analysis of the system developed, it is concluded that the system is reliable, maintainable and available for individual users’ consumption, commercial and industries. Some improvement can be added to the system in the future for the efficient functionalities and wide areas of application which include motion detection sensor integration, camera for surveillance and image capturing, addition of a biometric system for unique security identification together with the keypad and so on.

References

1. Hill J (2015) The smart home: a glossary guide for the perplexed.

2. Ajao LA, Ajao FJ, Adegboye MA, et al. (2018) An embedded fuzzy logic based application for density traffic control system, Int J Artif Intel Res 2: 6-13.

3. Aliyu S, Yusuf A, Umar A, et al. (2017) Design and development of a low-cost GSM-bluetooth home automation system. IJAIA 8:41-50.

4. Zhao Y, Ye Z (2008) A low cost GSM/GPRS based wireless home security system, IEEE Trans. Consum. Electron 54: 567-572.

5. Felix C, Jacob Raglend I (2011), Home automation using GSM, International Conference on Signal Processing, Communication, Computing and Networking Technologies 15-19.

6. Papadopoulos K, Zahariadis T, Leligou N et.al (2008) Sensor Networks Security Issues in Augmented Home Environment Proceedings of the IEEE International Symposium on Consumer Electronics, Las Vegas, NV, USA 1-4.

7. Abhishek AP, Joglekar A (2015) Implementation of home security system using GSM module and microcontroller IJCSIT 6: 2950-2953.

8. Yan M and Shi H (2013) Smart Living Using Blueooth-Based android smartphone, International Journal of Wireless Mobile Networks 5: 65-72.

9. Li RYM, Li HCY, Mak CK et al. (2016) Sustainable Smart Home and Home Automation: Big Data Analytics Approach IJSH 10: 177-198.

10. Ahammed T, Banik PP (2015) Home appliances control using mobile phone, Proceedings of 3rd International Conference on Advances in Electrical Engineering 251-254.

11. Mulla A, Baviskar J, Baviskar A (2014) DTMF based automation system with reduction of noise usinggoertzel DFT estimation, Fourth International Conference on Communication Systems and Network Technologies 1124-1129.

12. Yong Q, Hao L, Junhua H (2013) The Design of Grading Software System Based on Bluetooth in Android, 8th International Forum on Strategic Technology (IFOST) 16-19.

13. Huichenand L, Neil WB (2016) IoT privacy and security challenges for smart home environments MDPI Journal information, Basel, Switzerland 7: 1-15.

14. Bakoand A, Ali IA (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes, MDPI Journal Sensors 18: 1-17.

15. Khan SR, Dristy FS (2015) Android based security and home automation system. IJASA 3:15-24.

16. Sabeel U, Chandra N (2013) A Smart and Contemporary Home Security System using802.15.4 Standard. 5th International Conference on Computational Intelligence and Communication Networks 374-379.

17. Suh C, Ko Y (2008) Design and implementation of intelligent home control systems based on active sensor networks, IEEE Trans Consume Electron 54: 1177-1184.

18. Ping W, Guichu W, Wenbin X, et al. (2010) Remote Monitoring Intelligent System Based on Fingerprint Door Lock, International Conference on Intelligent Computation Technology and Automation.

Citation: Ajao LA (2018) A Smart Door Security-Based Home Automation System: An Internet of Things. SF J Telecommunic 2:2.