Vol. 10(36), Apr. 2020, PP. 4568-4582

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543

Design and Implementation of an RF Home Security System Prototype

Engr. Prof. Victor E. Idigo, Dr. (Mrs) Ifeyinwa Obiorah-Dimson, Engr. Tochukwu Churchill Akubue

Electronic & Computer Engineering Dept., Nnamdi Azikiwe University, Awka, Nigeria

***Corresponding Author's E-mail:** tochukwuakubue@gmail.com*

Abstract

This article presents a report on the prototype design of a Smart home RF security system using predictive analytics. An infrared transmitter sends 38KHz constantly to an infra-red receiver to form a security line. The moment a disturbance is detected, a trigger LED flash is activated and then an encoded RF signal is transmitted through a 433MHz RF Module to a latch decoder. A microcontroller verifies the exact security code and uses it to activate relay switches. This is connected to a USB cable into a computer with infused camera. A timer is then setup for less than 5secs in order to trigger the camera. The camera snaps for 90secs and stops while all the captured images on the scene are stored on the hard disk of the laptop for further analysis.

Keywords: *Radio frequency, home security, microcontroller, smart home, predictive analytics.*

1. Introduction

Security may be seen as freedom from, or resilience against, potential harm from external forces or protection from hostile forces. It can also be seen as the absence of harm; as the presence of an essential good; as secrecy; as containment; and as a state of mind. The term is also used to refer to acts and systems whose purpose may be to provide security. Smart Home also known as Automated Home or Intelligent Home explains a home where there is automation of daily tasks with electrical appliances. This could be the control of lights, fans, viewing of the house interiors for surveillance purposes or giving the alarm alteration or indication in case of gas leakage [3]. According to [11], home security is seen as both the security hardware in place on a property as well as personal security practices. Security hardware includes doors, locks, alarm systems, lighting, motion detectors, security camera systems, etc. that are installed on a property; personal security involves practices such as ensuring doors are locked, alarms activated, windows closed, extra keys not hidden outside, etc. Security is an important aspect or feature in the smart home applications [4, 6, 10]. The new and emerging concept of smart homes offer a comfortable, convenient, and safe environment for occupants. Conventional security systems keep homeowners, and their property, safe from intruders by giving the indication in terms of alarm. However, a smart home security system offers many more benefits [3, 6]. Most home security designs including some smart homes make use of CCTV cameras which keep continuous records of the environment thereby leading to privacy issues in addition to obtaining huge amount of video clips to be monitored or searched through for crime thus requiring an employee to always surf through these clips while others use alarms, password or

Article History:
Received Date: Apr. 15, 2019
Accepted Date: Aug. 05, 2019
Available Online: Apr. 01, 2020

facial/finger print enabled doors, etc. to scare or prevent the criminals from gaining access into homes. Criminals always find a way to disable these security features since the security systems are preventive mostly and the criminal is made aware of such systems. A smart home that is not primarily interested in alerting criminals that their presence has been detected but yet still obtaining evidence of the crime is most effective since the criminals are not certain of the security system in place. Finally, the cost implication of providing smart home is quite high and thus not affordable to the average home owner.

The aim of this work is to obtain an efficient design of an implementable prototype of a smart secured home which is capable of not only detecting intruders using smart sensors but smartly reconstituting the scene of a crime which law enforcement can use for criminal prosecution.

2. Literature review

Ref. [6] reviewed a smart home using the X10 protocol on Powerline Carrier Systems which allows coded signals travel on existing electrical wires in a home and then devices attached to such wires react to the codes or command that pass through these wires. This is a smart way of cost reduction in making an already existing home smart but it is challenged by the noise generated by the electrical lines as it powers other devices thus X10 device could interpret electronic interference as a command and react, or it might not receive the command at all.

Ref. [1] designed a secure smart home using microcontroller, SIM card enabled GSM module, alarm system, Ethernet, keypad, micro SD card, sensors and camera. The keypad is attached to the entrance door and is designed to open the door only when a correct code is supplied. On the reception of three consecutive wrong codes, a camera takes snap shots, stores in the SD card and using Ethernet transfers to cloud while activating alarms and sends SMS to the home owner and central security.

Ref. [9] presented a smart home automation system using a GSM module, Bluetooth application or a keypad to provide password facility for key based door locks. If an intruder tries all of the three methods of gaining access into the home consecutively without success, then Arduino controller alerts the home owner through SMS while initiating a buzzer alarm to scare away the intruder and alert neighbors.

Ref. [2] proposes an SMS-based home security system with immediate feedback. Here, a homeowner can control their home lighting and appliances using SMS messages from a pre-set registered mobile number. If the SMS is not from a legitimate mobile number, the system ignores the message. In the case of an intrusion, the appliance control subsystem and security subsystem in the proposed system informs the owner through SMS.

Ref. [7] went on to propose a secure smart home using biometric image capture for access authorization. It may be done in conjunction to a smart phone access application through Bluetooth.

Ref. [5] used a smart phone application running on Bluetooth technology to control up to 18 devices in a smart home. The system comprise of Arduino board, Bluetooth module, smart phone, ultrasonic sensor and moisture sensor.

Ref. [8] also designed a smart home based on a Bluetooth enabled Arduino microcontroller and an Android application. The system was able to control light intensity, DC motor speed and DC servomotors.

3. Research gaps

The literatures reviewed implemented a secure smart home using different and diverse methods ranging from pass code enabled door to voice call access control. Amidst the advantages obtainable from these different security systems, some gaps have been observed.

- ✓ Passing commands through power lines is not an excellent way of sending out communication to devices because of the noise generated by the electrical lines as it powers other devices thus X10 device could interpret electronic interference as a command and react, or it might not receive the command at all.
- ✓ The cost of obtaining an affordable smart home is always on the high side thereby discouraging home owners from buying into this technology.
- ✓ Password enabled systems, SMS alert and alarm alert systems have challenges not limited to the following; alerting a user about an intrusion attempt by SMS is never a good practice. Users may not check their phones for SMS messages frequently, or may not be near enough to the phone to hear a message received tone, so they could easily miss the intrusion alert. This work provides limited security, as they only use cameras and no other security mechanisms. The password to the door can easily be gotten through social engineering especially as this code is used by the user every day thus he may be careless with it or the attacker can use a sophisticated means to bypass the password. Finally, the use of alarm system barely scares the criminal element away while he taking notice of the security system, returns better equipped to beat the system.
- ✓ Bluetooth has a maximum communication range of 100m in ideal conditions. More may be needed in a smart home environment. Also, Bluetooth communication has comparatively high power consumption, so the batteries of devices need to be frequently recharged or replaced. Even with the use of Bluetooth Low Energy (BTLE) technology, which provides the same range of communication, security concerns such as eavesdropping and weak encryption arises. This article mainly focuses on the security of a home when the user is away from the place.

This security system uses web cameras, installed in house premises, which are operated by software installed on the PC while the obtained images or video of intruders can be handed over to law enforcement for security audit.

4. Methodology

This work used embedded system and prototyping methodology to achieve its aim. The design phase is divided into two phases; the hardware design and interfacing subsystem, the control software subsystem.

A. Hardware design and interfacing subsystem:

This section presents the design of a complete control scheme for the smart home security system incorporating all the hardware needed.

1) *PIC 16F873A Microcontroller:* This Edge PIC controller presents a low cost device with high clock speed running at the rate of 20MHz, 4K*14 words of FLASH program memory,

192*8 bytes of data memory (RAM), 128*8 bytes of EEPROM data memory and this is enough for the sensing application. An Edge PIC controller executes most of its instructions in 0.2micro seconds or 5 instructions per microseconds. Its speed in instruction execution is high. The efficiency and accuracy is very high. The instruction set consists of 35 single-word instructions. This is used at the disturbance detection and sending section of the system. It controls the latch encoder, the RF Module at the sending section, the IR Tx and Rx. It is also responsible for the generation of the S-Pulse signal of 38 KHz used by the IR Tx.

2) *PIC 16F877A Microcontroller:* Edge PIC controller presents a low cost device with high clock speed running at the rate of 20MHz, 8K*14 words of FLASH program memory, 368*8 bytes of data memory (RAM), 256*8 bytes of EEPROM data memory and this is enough for the control application. An Edge PIC controller executes most of its instructions in 0.2micro seconds or 5 instructions per microseconds. Its speed in instruction execution is high. The efficiency and accuracy is very high. The instruction set consists of 35 single-word instructions. This is used at the receiving section of the system. It controls the latch decoder, the RF Module at the receiving section, the LCD display and the relay switches. It is also responsible for the predictive control of the system.

   The reasons for choosing these two microcontrollers are their low cost but yet high clock speed, wide availability for purchase, large user base, extensive collection of application notes, availability of low cost/free development tools and easy serial programming (and reprogramming with flash memory, thus non-volatile) capability. They have simple core architecture with code optimization, linking, routing, fitting and placement. They have fine grained ADCs as well as set of registers that function as general purpose RAM. They also have special purpose control registers for on-chip hardware resources which are also mapped into the data space. The EDP PIC code space when implemented as FLASH ROM enables Many Time Programmability (MTP).

3) *PSU*: A micro power supply was developed. This was built using rectifiers (4*1N4001), filters (470μF) and voltage regulators (7805). Starting with an AC voltage, a steady DC voltage is obtained by rectifying the AC voltage which after is filtered to a DC level and finally regulated to obtain a desired fixed DC voltage. The regulation is usually obtained from an IC voltage regulator unit, which takes DC voltage and provides sufficient lower DC voltage, which remains the same even if the input DC voltage varies, or the output load connected to the DC voltage changes. Fig. 1 depicts the working of the power supply unit sowing the transformer which steps down the 230V from AC main, the diode rectifier which converts the stepped down AC voltage to DC voltage, the capacitor helps in smoothing the obtained DC Voltage while the 7805 regulator provides sufficient DC voltage while regulating it against voltage/load variation.

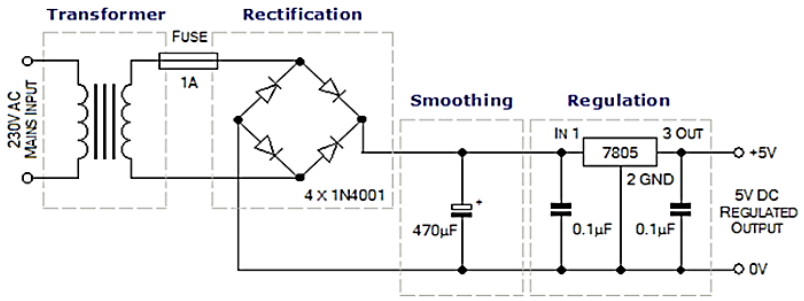

Figure 1: Micro-power supply unit showing the components embedded in it

LCD display: This is an LMO16L LCD display connected to the PIC 16F877A controller to display the status of the system informing of when the system is powered ON, when there is a breach in security, when the camera is taking snap shots and when the camera is in idle state. It is a 14 pin LCD display with 1 controller which can support 80 characters. It has a Module dimension of 80.0 x 36.0mm, viewing area of 66.0 x 16.0mm, character size of 2.96 x 5.56mm, dot size of 0.56*0.66mm and a weight of about 35g. Fig. 2 shows the LMO16L LCD display discussed here. It has 1 controller and 14 pins with extra 2 pins for back-light LED connection. **Fig. 2.**

Figure 2: 14 pin LMO16L LCD display

4) *Camera*: This can be any web camera. The work used the web camera infused to the laptop that serves as the storage server.
5) *Storage*: The storage used for this design is the Hard disk (My document folder) of the laptop used as the storage server. The relays are connected to a USB cable which is connected to the USB port of a laptop. When these relays are activated, they in turn activates the USB connection thereby turning ON the web camera of the server laptop which takes snap shots of the affected area and stores in the hard disk of the laptop. This can be seen in fig 3. showing the camera snapshot folder of the Hard disk of a computer storing snap shots from a compromised area. It should be noted that the My Document folder is the default storage location except when changed.

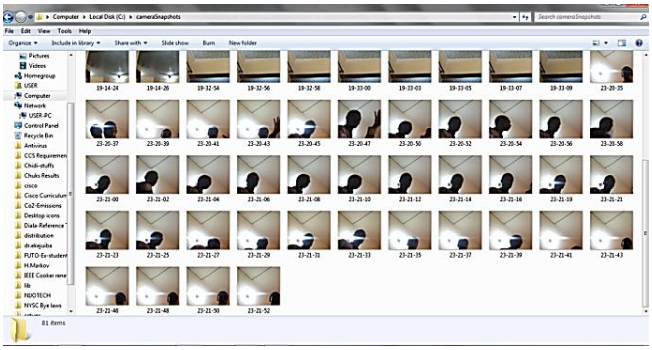

Figure 3: Captured snap shots saved in PC

6) *Infrared Transmitter and Receiver*: The TSOP1738 Infrared receiver built with PIN Diode, Preamplifier and internal filter for PCM (Pulse Code Modulation) frequency is used. It operates on a carrier frequency of 38 KHz. It is a Photo Detector, IR Filter with shielding against EMI or RFI interference as well as being CMOS and TTL compatible. It also has active low output, immunity against ambient light, low power consumption and is able to transfer data continuously up to 2400bps at a supply voltage range of 4.5 – 5.5V. While TSAL6200940 nm emitting diode in GaAlAs multi quantum well (MQW) technology with high radiant power and high speed moulded in a blue-gray plastic package Infrared transmitter was used for the sensing section. It has high reliability, high radiant power, high radiant intensity, low forward voltage and is suitable for high pulse current operation. Fig. 4 below shows the sensing section with the IR Tx and Rx facing one another sending and receiving signals on the 38KHz frequency thereby forming a Line of Sight Cloud Wave (LWC = 1).

Figure 3: Infra-red transmitter & receiver forming a line of sight

7) *RF Module*: This design made use of two FS1000A 433MHz RF wireless transceiver module to synchronize the communication between the sensing section and the controller section. The receiver operates at 5VDC, with a current of 4mA, a receiving frequency of 433.92MHz and receiving sensitivity of -105DB while the transmitter operates on a voltage of 3.5-12V, transmitting distance of 20-200 meters, transfer rate of 4kbps, transmitting power of 10mW and transmitting frequency of 433MHz.

8) *Latch Encoder*: This HT12A latch encoder is a low power and high noise immunity data encoder built with CMOS technology and operating at a voltage range of 2.4 - 5V and a low standby current of 0.1mA at a VDD of 5V. It has a 38 KHz carrier for infrared transmission medium, minimum transmission word of one word, 18-pin DIP, 20-pin SOP package. It is used to encode the information that will be sent from the sensing section to the control section.

9) *Latch Decoder*: This HT12D latch decoder is a low power and high noise immunity data decoder built with CMOS technology and operating at a voltage range of 2.4-12V and at low standby current. It is capable of decoding 12 bits of information obtained through 8 address bits and 4 data bits. It also has 18-pin DIP, 20-pin SOP package. This is used to decode the encoded information sent from the sensing section of the control section.

B. Control software design:

This section presents the implementation of the embedded Model Predictive Controller using a PIC 16F877A (latch decoder and relay switching section) and PIC 16F873A (IR Tx-Rx section) microcontrollers for its implementation. The control codes written to the PIC 16F877A is shown in appendix 1 while that written to PIC 16F873A is shown in appendix 2.

5. Description of operation functionality

The working of the security monitoring and control system is as follows; the Infrared (Tx & Rx) sensors (both connected to the PIC 16F873A microcontroller) are installed at doors and windows. This section of the system is powered by a 9V battery. Once the system in ON, the trigger LED light on the receiving section flashes once to indicate readiness while the PIC 16F873A Microcontroller (S-Pulse generator) generates 38KHz frequency and activates the IR Tx to commence sending infrared signals on 38KHz frequency to the IR Rx. This generates a Line of Sight Wave Cloud (LWC=1).

It should be noted that only infrared signal modulated at 38 KHz will be monitored by the IR Tx & Rx. Upon a disturbance of the LWC, the IR Rx will not receive a signal thus LWC=0. Since the IR Rx sensor is connected to the PIC 16F873A microcontroller, it activates an LED to indicate signal disturbance while sending a signal informing of a breach of LWC. The PIC 16F873A microcontroller activates the Latch Encoder (HT12A) to encode the signal and then the PIC 16F873A microcontroller sends the encoded signal to the PIC 16F877A microcontroller on the receiver section through the RF 433MHz transmitter module.

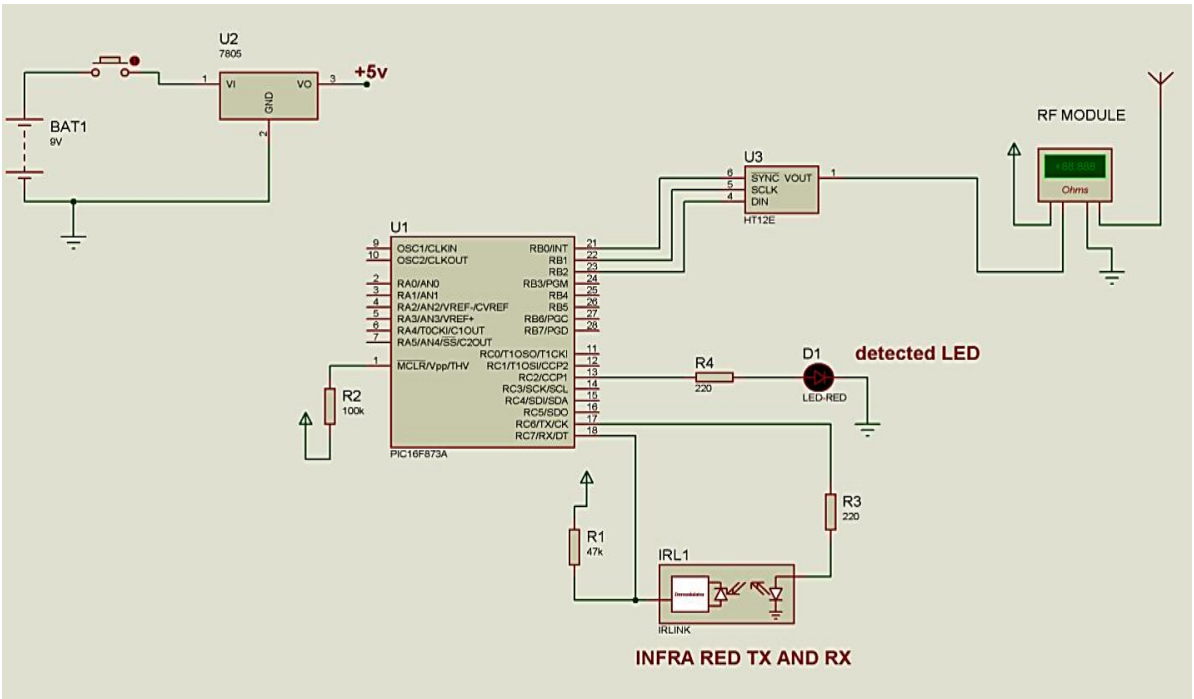

Figure 5: The transmitting section

Fig. 5 shows the transmitting section. The topmost left side depicts the 9V battery power supply source for this section. The IR Tx and Rx forming a line of sight are connected the PIC16F783A for pulse generation and feedback signal respectively. Upon an invalid feedback signal, the PIC16F783A

sends a breach of security signal to the receiving section through the HT12A encoder and the RF module.

At the receiving section as depicted in fig. 6, the RF 433MHz receiver module receives the encoded signal on the 433MHz band and sends it to the PIC 16F877A microcontroller which activates the LCD display (LMO16L) with a message for signal reception. The PIC 16F877A microcontroller then sends the received signal to the Latch decoder (HT12D) for the decoding of the received signal. The Latch decoder communicates the PIC 16F877A microcontroller with the decoded signal. This is checked for validity of true intrusion or otherwise. If the signal is valid, then the PIC 16F877A microcontroller sends a Camera ON message to the LCD display while activating the four relays connected to the USB cable in order to activate the camera infused Laptop for taking snap shots for 90sec.

After snapping for 90secs, the relays are deactivated while the snapped pictures are saved to the Hard disk of the connected Computer. This process is repeated as long as LWC=0; in other words, if the IR Tx and Rx continues receiving a disruption in their signal (LWC = 0), after the first batch of snapping process, then the camera infused laptop is activated again for more snapping cycles for as long as there is disruption in the IR sensing section.

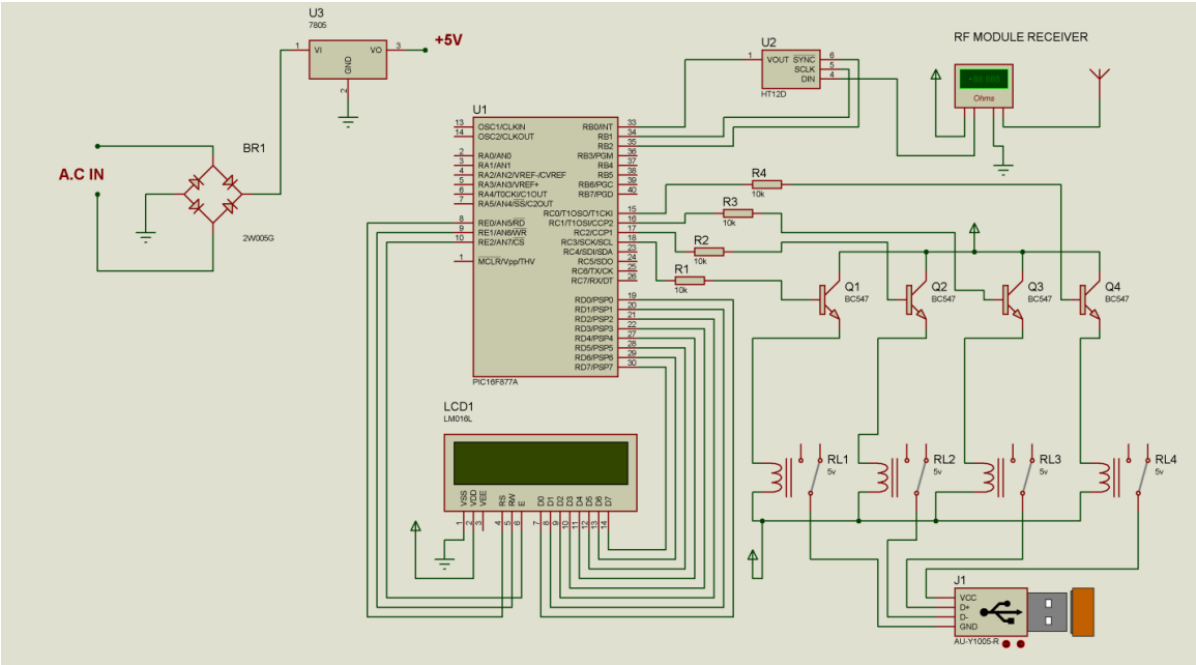

Figure 6: The receiving section

Fig. 7 gives the entire system overview highlighting how each system component or section is connected to other sections. The process flows from the micro power supply which powers the PIC16F873A microcontroller. This microcontroller in turn enables the IR Tx to send signals to the IR Rx on the 38KHz frequency. The Rx sends a feedback signal to the microcontroller upon reception of signals from the Tx thus forming a line of sight. The Rx encodes signal from the Tx and sends to the PIC16F877A through an encoder, an RF transceiver (on the 433MHz frequency) and a decoder for message encoding, transmitting and decoding. The PIC16F877A checks for validity of the received signal or otherwise by comparing it with predicted signal output and activates the camera to take snap shots and store if breach signal is valid.

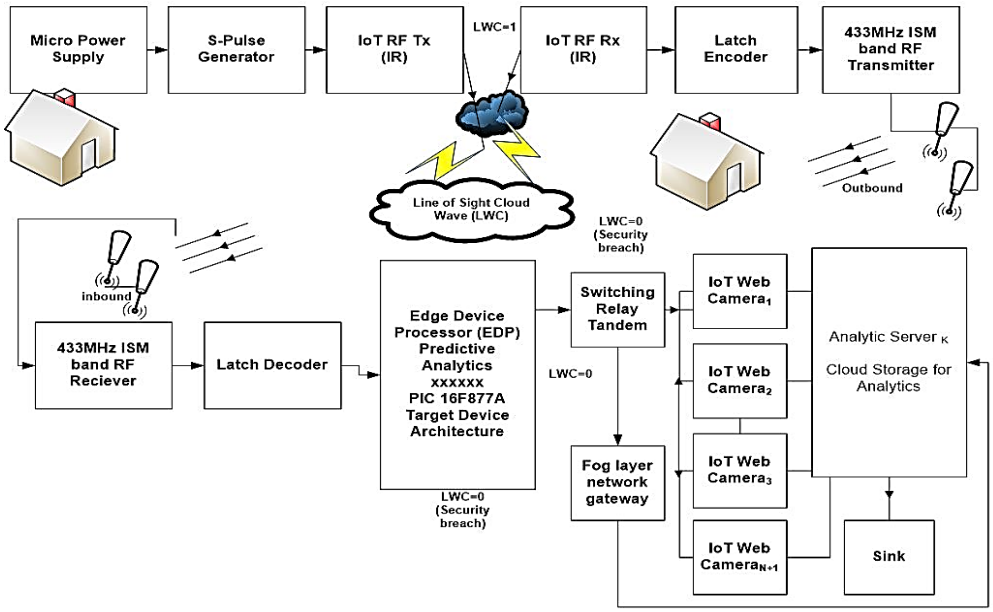

Figure 7: Global system architecture

Fig. 8 shows the LCD display giving the status of the security system during different situations that is at the system default state (left side) and at the state when there is a security breach and the web camera is turned ON to take snap shots.

Figure 8: LCD displays

The cost of production of this system without the use of a laptop as the source of camera and offline storage but using an IP camera and online storage location is as in table 1.

Table 1: Cost analysis of system production

S/N	Item	Price
1	PIC16F873A	950
2	PIC16F877A	1,500
3	RF Module	3,500
4	Encoder	700
5	Decoder	700
6	IR Sensors	350
7	LCD	850
8	PSU	1900
9	Vero board	200
10	P2P IP Camera	12,800
11	SD Card (optional)	4,700
12	Wires, soldering led, resistors,	1,200
13	Packaging	2,500
	Total	**31,850.00**

6. Result analysis

This system once powered ON sends valid signals from the sensing section to the receiving section thus creating a predictive history of a secure home. As other signals arrive the receiving section, they are compared to the predictive history for prediction differential or otherwise. If there exists no prediction differential, then the home is still safe and the signal is saved as part of the predictive history but if a differential exist, then a breach of security is assumed. Also, a disruption of the line of sight leads to the receiving section obtaining an invalid or nil signal; this section uses predictive analysis within 5 seconds to determine the validity or otherwise of the disruption thus activating secured web cameras for obtaining the snap shots of the crime screen. These stored data can be used to reconstitute the crime scene and used as evidence for criminal justice. The system can display the status of the home as secure, having invalid breach or under siege of crime.

7. ACKNOWLEDGEMENTS

The authors are grateful to all those that contributed to the successful realization of this work.

Conclusion

This paper explained the concept of security, home security and the smart home while paying attention to the security segment of a smart home. It also reviewed related works in the field, highlighting their methodologies, pros and limitations. The Authors of this paper proposed and implemented the prototype of an effective smart home using simple components making it easy to build and consequently of low cost. The work successfully established a line of sight security perimeter, uses predictive history to validate a true or false intrusion; auto activates a camera in less than 5 seconds for crime scene capture and storage only when a true intrusion is validated while displaying the status of the home security on an LCD segment. This system is recommended for use in places that requires the absence of human being except for some special occasions like the bank strong room. Instead of using a CCTV system that keeps recording continuously and over burdening the cameras and storage unit, in addition to requiring that an analyst may have to go through a large number of files to detect the exact crime scene, this system would only turn ON the cameras when a true intrusion is detected as well as keep a lesser quantity of video clips which would actually be the exact needed video clips for the crime analysis.

This system is designed as a proof of concept for a broader security system which is proposed to have more features in addition to having the ability to make the stored pictures available in cloud storage so that the user can access the pictures or video remotely even as the crime is on-going. The user is alerted about disturbances in his home to allow him call the security team to surrender the criminal(s) while in the act or go after them using the evidence of the crime. PIR sensors can also be used for detecting human presence, the vibration sensor and magnetic door contact sensor installed at the windows and doors are used for detecting window breaking and door opening.

Future research works to improve this article should focus on including features which enables the camera obtain very good images at night or in dark areas and yet the obtained image will provide good image details as if it were taken during the day. Cloud storage of snapped image files, remote user access to stored pictures as well as the system initializing a call to the home owner and law enforcement agency during an active crime can be included as improvement to this system.

References

[1] E. Isa, and N. Sklavos, "Smart home automation: GSM security system design & implementation," *Journal of Engineering Science and Technology Review*, vol. 10, no. 3, pp. 170-174, 2016.

[2] I. Azid, and H. Sharma, "Intelligent home: SMS based home security system with immediate feedback," *World Academy of Science, Engineering and Technology*, vol. 72, pp. 934-937, 2012.

[3] J. Bangali andA. Shaligram, "Design and implementation of security systems for smart home based on GSM technology," *International Journal of Smart Home*, vol. 7, no. 6,pp. 201-208, 2013.

[4] M. Ab-Rahman and M.Razaly, "A review of security system for smart home applications," *Journal of Computer Science*, vol. 8, no. 7, pp. 1165-1170, 2012.

[5] M. Asadullah and K. Ullah, "Smart home automation system using Bluetooth technology," 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, Pakistan, May, 2017.

[6] R. Robles, and K. Tai-hoon, "A review on security in smart home development," *International Journal of Advanced Science and Technology*, vol. 15, pp. 13-22, 2010.

[7] S. Chitnis, N. Deshpande and A.Shaligram, "An investigative study for smart home security: issues, challenges and countermeasures," *Wireless Sensor Network*, vol. 8, pp. 61-68., Published Online April 2016 in Scientific Research publishing.

[8] S. Das, S. Ganguly, S. Ghosh, R. Sarker and D. Sengupta, "A Bluetooth based sophisticated home automation system using smartphone," 2016 International Conference on Intelligent Control Power and Instrumentation (ICICPI), Kolkata, India, pp. 236-240, February, 2017.

[9] S. Umbarkar, G. Rajput, S. Halder, P. Harname and S. Mendgudle, "Keypad/Bluetooth/GSM based digital door lock security system," *Advances in Intelligent Systems Research*, vol. 137, pp. 749-757, 2017.

[10] W. Ali, G. Dustgeer, M. Awais and M. Ali, "IoT based smart home: Security challenges, security requirements and solutions," 23rd International Conference on Automation and Computing (ICAC) 1st, Huddersfield, UK, pp. 5772-5780, September, 7-8, 2017.

[11] *"Top Industry Trends for Home Security in 2018,"* Industry Trends for Home Security. January 12, 2018. Retrieved from http://www.smartfence.in/blog/top-industry-trends-home-security-2018/

Appendices

Appendix I:

The transmitter codes for the PIC 16F873A

```
// survellance type 2
#include <htc.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h> // used to check if xter is printable ascii or not i.eisprint(c)

__CONFIG(XT & WDTDIS & PWRTEN & BORDIS & LVPDIS & WRTEN & DEBUGDIS & DUNPROT &
UNPROTECT);
__IDLOC (EEC1);
#define ir_tx RB7
#define ir_rx RB0
#define detected_led RC4
#define tx_pulse RC3 // active low
// function prototypes
void delay (long x);
voidinit ();
void set_up_timer1();
void main ()
{
INTCON = 0X00;
init ();
 set_up_timer1();
 TMR1ON =0;
while (1)
{
if (ir_rx ==1)// ir sensor hasnt detected infra red pulses. its blocked
 {
detected_led =1 ;// put on the detected led
tx_pulse =0; // active low
  //TMR1ON =1;
delay (10000);
tx_pulse =1; // active low
delay (10000);
tx_pulse =0; // active low
delay (10000);
tx_pulse =1; // active low
 // while (TMR1IF ==0)
 // {
   // Wait
// }
while (ir_rx ==1)
  {
   // wait to become hi
  }
detected_led =0 ;// put off the detected led
 }
else
 {
```

```
detected_led =0 ;// put off the detected led
tx_pulse =1; // active low
 }
}
}
// functions are here
voidinit()
{
 TRISA = 0x00;// relay to usb is here
 TRISB = 0x01;// rb0 = rx in via irrx sensor
 TRISC = 0x00;//
 ADCON1 =0X06; // NO ADC ON PORTA
 PORTB = 0X00; //
 PORTA =0X00;
 PORTC =0X00;
 //
tx_pulse =1; // bcosits active lo
ir_tx =0; //ir_tx should be on
}
void delay (long x)
{
for ( ; 1 < x; x--);
}
void set_up_timer1()
{
 T1CON = 0B00111100; // prescale value = 1:8
 TMR1IF = 0;// ENSURE FLAG IS CLRED I.E PIR1,TMR1IF
 TMR1H = 0X0B;
 TMR1L = 0XDB; // if u want 0.5 sec
 TMR1ON = 1;
}
```

Appendix II:

The control codes for the PIC 16F877A

```
// surveillance type 2
#include <htc.h>
#include <stdlib.h>
#include <string.h>
//#include <ctype.h> // used to check if xter is printable ascii or not i.eisprint(c)

__CONFIG(XT & WDTDIS & PWRTEN & BORDIS & LVPDIS & WRTEN & DEBUGDIS & DUNPROT &
UNPROTECT);
__IDLOC (EEC1);
#define ir_tx RB7
#define ir_rx RB0
#define detected_led RC4
#define tx_pulse RC3 // active low
// function prototypes
void delay (long x);
voidinit ();
void set_up_timer1();
```

```
void main ()
{
 INTCON = 0X00;
init ();
 set_up_timer1();
 TMR1ON =0;
while (1)
{
if (ir_rx ==1)// ir sensor hasnt detected infra red pulses. its blocked
 {
detected_led =1 ;// put on the detected led
tx_pulse =0; // active low
  //TMR1ON =1;
delay (10000);
tx_pulse =1; // active low
delay (10000);
tx_pulse =0; // active low
delay (10000);
tx_pulse =1; // active low
 // while (TMR1IF ==0)
 // {
   // Wait
// }
while (ir_rx ==1)
  {
   // wait to become high
  }
detected_led =0 ;// put off the detected led
 }
else
 {
detected_led =0 ;// put off the detected led
tx_pulse =1; // active low
 }
}
}
// functions are here
voidinit()
{
 TRISA = 0x00;// relay to usb is here
 TRISB = 0x01;// rb0 = rx in via irrx sensor
 TRISC = 0x00;//
 ADCON1 =0X06; // NO ADC ON PORTA
 PORTB = 0X00; //
 PORTA =0X00;
 PORTC =0X00;
 //
tx_pulse =1; // bcosits active lo
ir_tx =0; //ir_tx should be on
}
void delay (long x)
{
```

```
for ( ; 1 < x; x--);
}
void set_up_timer1()
{
 T1CON = 0B00111100; // prescale value = 1:8
 TMR1IF = 0;// ENSURE FLAG IS CLRED I.E PIR1,TMR1IF
 TMR1H = 0X0B;
 TMR1L = 0XDB; // if u want 0.5 sec
 TMR1ON = 1;
}
```

Authors

Engr. Prof. Idigo V. E. received his M. Sc. in Engineering and Ph. D. in Communication Engineering. He is a corporate member of the Nigerian Society of Engineers (NSE), Member of the Institute of Electrical and Electronic Engineering (IEEE), USA, member of Council for the Regulation of Engineers (COREN) and a member of the International Association of Engineers (IAEng). He is currently a Professor with the Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. He was a lecturer at the Institute of Management and Technology (IMT), Enugu and also at Federal Polytechnic, Oko. Areas of his research interests include telecommunication, wireless sensor network, radio and television transmission, Computer Aided Designs etc. He is the incumbent Dean of the Engineering Faculty, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.
email: ve.idigo@unizik.edu.ng
Phone Number: +234-80639813480

Engr. Akubue T. C. recieved his B. Engr. degree in Computer Engineering from Enugu State University of Science and Technology (ESUT), Enugu State, Nigeria. He is a corporate member of Nigerian Society of Engineers (NSE), associate member of the Computer Professionals' registration council of Nigeria (CPN) and member of Council for the Regulation of Engineers (COREN). He is currently a post graduate student of the Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Areas of his research interests include digital control, artificial intelligence, real-time embedded and distributed systems, intelligent systems and program development.

email: tochukwuakubue@gmail.com
Phone Number: +234-8034971026