Journal of Engineering Sciences
Assiut University
Faculty of Engineering
Vol. 47
No. 6
November 2019
PP. 807–821

ECONOMIC WIRELESS HOME SECURITY SYSTEM USING IOT MODULE

Eslam F. Galal [*], Moataz M. Elsherbini and Hala M. Abdel-Kader

Depart. of Electrical Eng. at Shoubra, Faculty of Engineering, Benha University

Received 10 June 2019; Accepted 2 July 2019

ABSTRACT

Human Security against the risks of burglary, gas Leakage, and fire accident is the main objective of this research. This paper demonstrates the design and Implementation of IoT based security system in buildings via Node MCU and Blynk server with WiFi network connectivity. This system comprises wireless slave sensor nodes and a master controller node. Remote user alerts, portability, configured by the user and power saving and reliability are the main features of our proposed system. WiFi enabled IoT module processes the sensor-based events and transmits the sensor status to the controller. Upon receiving the event notification, the controller alerts the user locally by alarm a siren and remotely via notification, email using Blynk mobile application, phone call and SMS using GSM module. The IoT module makes the node small-size, cost-effective and easy to use. The proposed system is globally monitored and controlled.

Keywords: Security System, Wireless sensor network, NodeMCU, WiFi, Blynk Server, Internet of Things, Blynk mobile application, GSM.

1. Introduction

Nowadays, Guaranteeing security and safety of human have become an unavoidable necessity. Developments in smart home automation and embedded system fields must not only depend on providing a luxurious and a comfortable way to control homes remotely but also serve human security from exposure to dangers of burglary, gas leakage and fire accidents. The main advantage of smart homes is the security system with a variety of sensors to detect any suspicious issues threaten human. Security systems used also in industrial and public objects. Commercial companies offer security systems category as wired, wireless or mixed but so expensive for the common man in the Middle East to get, From here the demand for economic security system has emerged, because it must be available for many people since human security is inevitable. The wired system is not suitable for inhabited homes because of its destruction of walls, decoration, and needs preinstalled infrastructure. When the sensor nodes being wireless, they can be easily placed anywhere inside the building, thus it achieves portability in the deployment, easy installation of Wireless system. Having WiFi availability is an added advantage for any system. Hence, Data can be brought from anyplace and it very well may be moved to cloud for capacity and observing. Advanced security systems can provide the data to the user remotely using a hybrid communication system which includes IOT, mobile communication methods.

Low power consumption is the main selection criteria for wireless network nodes.

2. Literature survey and drawbacks

In [1]. using Raspberry Pi with WiFi network and wireless sensor nodes which enable a camera for surveillance, the system expensive and don't use a mobile application. Semanur KARACA et.al. 2016 using an embedded server with Wireless sensor network, each node includes separate ESP8266 WiFi module, ARM microcontroller that not reliable and also difficult to interact to the system throw webpage with entering IP [2]. M Akhil Raja et.al. proposed Using of Arduino and GSM module along with monitoring sensors, ESP8266 WiFi module, and its sensor connected by wire to Arduino and don't illustrate how to interact with the system using WiFi module [3]. Using Arduino Uno and home monitoring sensors with an android mobile application don't show how to interface the hardware with the mobile application and its local control only, also centralized around Arduino board (Aadel Howedi et.al. [4].). Using Arduino Microcontroller, a cloud server for the remote control through internet by mobile application, a GSM shield for the remote control through cell phone SMS and a variety of sensor, sensors connected by wire to Arduino, connected to Router using LAN cable with Ethernet shield, there isn't option to control system manually if mobile failed [5]. Md ShariqSuhail et al In [6]. Using Raspberry Pi, Arduino mega and GSM module and Webcam to capture an image and send mail to a user, the system is expensive and also sensors connected by wire to Arduino, don't use a mobile application to control system. Per [7]., using Arduino mega, V3 voice recognition and ESP8266 Wi-Fi module and sensors which connected by wire to Arduino mega, local control only, a mobile application doesn't demonstrate, there isn't an alternative communication method to control the system. using Raspberry Pi 3, sensor nodes each include Arduino Nano boards and NRF24L trans-receiver, with an MQ Telemetry Transport (MQTT) channel described in [8]., The maximum number of nodes is limited to eight, Dynamic mesh networking is not available in the System, There is no physical hardware address present for the nodes, there isn't another way to control the system during internet failure, there isn't manual control option. Using Galileo gen2 board, servo motor, sensors, and android applications which connected using WiFi to Galileo gen2 board for monitoring and control, there is lack of remote monitoring, the mobile application isn't demonstrated, and there isn't another way of communication in [9]. Dr. M.L. Ravi Chandra, B. Varun Kumar proposed a Raspberry Pi 3, security sensors, a camera to captures the picture and sends it over mail, IoT web server, there isn't mobile application to control system , there isn't an alternative communication method, Raspberry Pi 3 connected to Router using LAN cable, sensors connected to the Pi by wire [10].

3. Proposed system

All the drawbacks introduced in the previous work will be developed and revised by our proposed security system, using wireless sensor network based on NodeMCUs (IoT/WiFi modules) which integrates sensor alerts with Bylnk server, GSM module. NodeMCU is a low cost, reliable, compact which integrates the ESP8266 WiFi module with a microcontroller in a single board. The system based on WiFi connectivity. Here, we use a WiFi module for wireless transmission instead of Zigbee since it has long range and high bandwidth. Wireless sensor nodes can be easily installed anywhere inside the home. The aim of our paper is to design and implement an economic, reliable, energy efficient, long range, globally accessible security system using NodeMCUs (IoT Modules), and GSM

Modem and Blynk server to alert the user about the intrusion, gas leakage, fire, burglary. The proposed system block diagram is shown in [Figure -1].

4. System architecture

Figure-2 shows the detailed architecture of IoT based wireless security system. The system divided into three parts:

- Local hardware.
- Web server (Blynk cloud).
- Smartphone with internet capability.

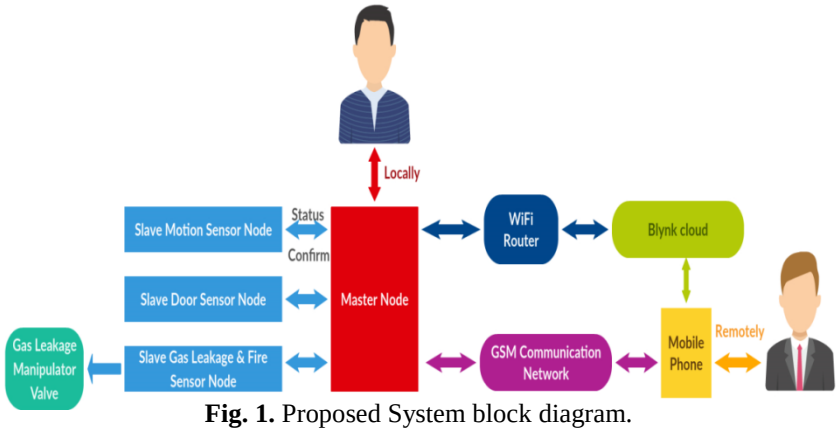

Fig. 1. Proposed System block diagram.

4.1. Local hardware is divided into three parts:

- WiFi-enabled sensor nodes (slave nodes)
- Controller node (Master node)
- IP Camera

A. WiFi-enabled sensor nodes (slave nodes)

Each node comprises a sensor, NodeMCU (ESP8266). NodeMCU is an economic open source WiFi module used for IoT applications. The IoT module will process the sensor output and transmit the sensor status to the master node via WiFi. There are three types of sensor nodes in the system. Motion (PIR) sensor node and MQ-5 Gas leakage sensor, LM35 Fire sensor node and Door Reed magnet and switch sensor node. PIR node will detect the intruder. Gas leakage, Fire detection included in a node to detect gas leakage, triggers a buzzer and activates the gas safety device i.e.; a solenoid valve (Shut-off Valve) which closes the Household Gas Pipeline or detects fire, triggers a buzzer. Door node detects the door opening.

B. Controller node (Master node)

It is built on NodeMCU, comprises GSM for remote notification and Control, Keypad for Arm/Disarm the system/change password, LCD for visualization option and buzzer for emergency alert. This node responsible for receiving the status of each sensor node based event, send a notification to Blynk mobile application, email notification to the user through internet and dial, send SMS to a preset mobile number using the GSM, alarm the buzzer. The user can monitor, control the system from anywhere via Blynk application or send SMS.

C. IP Camera

Used to surveillance the home when any suspicious event happened and to confirm any false alarm using the pre-developed mobile application through internet connection using WiFi.

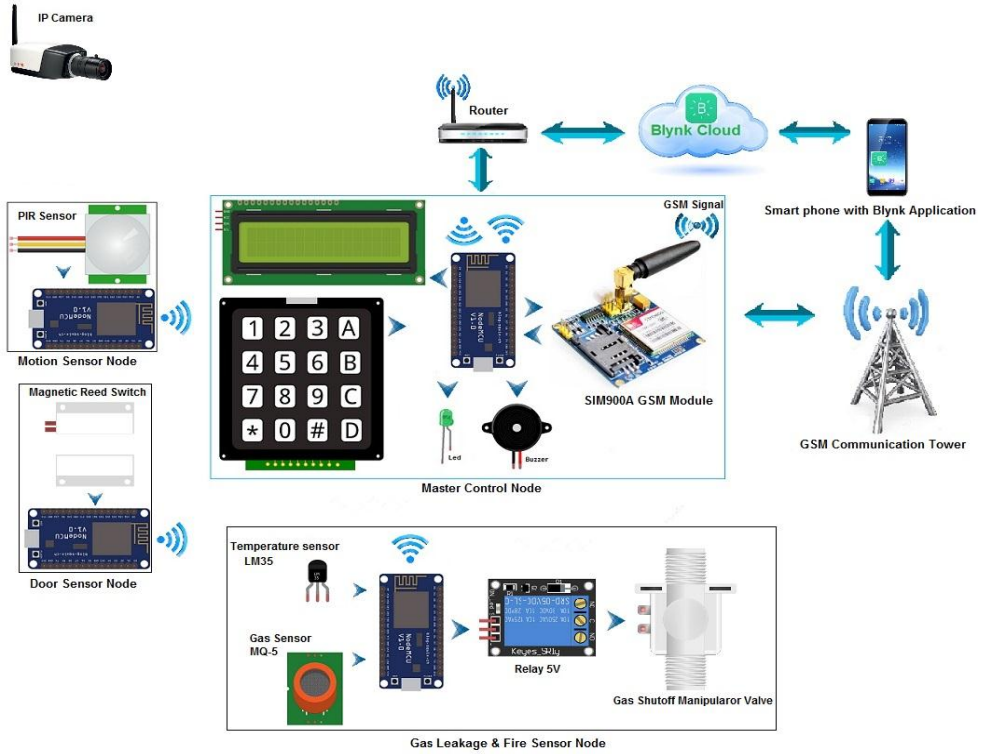

Fig. 2. Proposed System Architecture

4.2. Blynk server

Its open-source server used to connect the system master controller node with the Smartphone-based Blynk mobile application through the internet, handle data transfer between them as shown In [Figure-3].

4.3. Smartphone with internet capability

Used to get alerts from the GSM module SIM900A when there is an abnormal event in the house such as an intrusion or fire or gas leakage. It is also used to send SMS commands to the Controller node to control the Security system ON/OFF or know its status at real time. Used to get an email notification, alert notifications via Blynk mobile application which used to monitor the state of the home and also to control the security system ON/OFF via Blynk server from any place through the internet. In [Figure-4] the user diagram of the system and shows the tasks that the user can perform.

Fig. 3. Blynk server

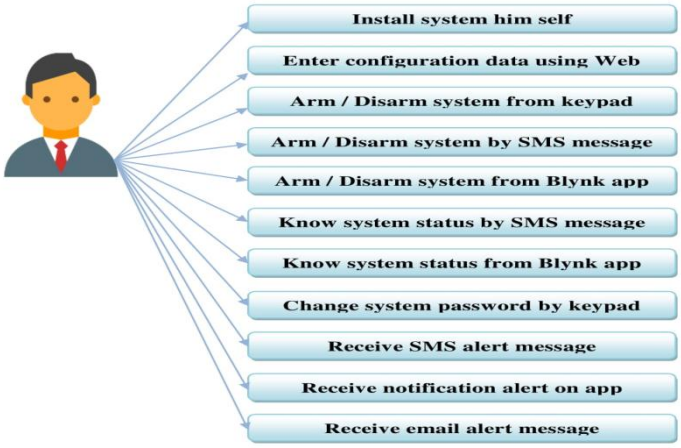

Fig. 4. User diagram of the system

5. System design and advantage

During the design of the system, we encountered problems and were Solved as follows:

– Overcome the need for a router in communication between Master and Slave sensor nodes.

The master NodeMCU work as an access point to the slave nodes, while each slave node works as a station (client), connected with the master node (access point) using WiFi connectivity.

– Eliminating the IP-addresses conflict with other Projects.

The access point (AP) has a fix IP address. The Station (Slave Sensor Node) uses this Predefined IP to connect to the AP.

– Reduce the time spent by each Station to be connected with the Access point.

Configured slave node (station) to use static IP addresses and hard-coded Gateway and Mask, to reduce the time spent in connecting to the AP. Instead of the access point, DHCP distributes IP-addresses for Slave nodes, using static network configuration to win time by not waiting for access point DHCP.

– Overcome limitations of the number of clients can connect to Access point NodeMCU module.
– Change maximum connection defaults of the Master node by programming and hard-coded.
– The master node maintains monitoring Slave Sensor nodes network and connects to the Blynk cloud to send events alerts to the homeowner globally.

The master node configured in both access point (AP) mode and station (ST) mode (AP_ST) mode. It works as an access point (AP) to monitor, communicate with slave sensor nodes locally, receives its status. Only when an event happened, Master node Works as a station (ST) to communicate with the home router to get access to the internet network and connects to Blynk cloud to send the notification and email alerts to the user Blynk mobile application remotely. Then disconnect from the cloud, back again to access point (AP) mode to monitor slave nodes, as shown In [Figure-5].

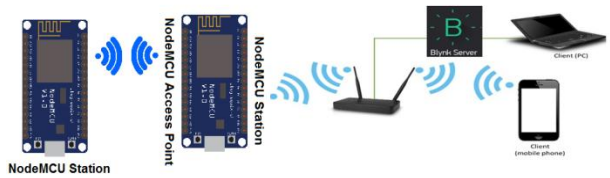

Fig. 5. NodeMCU switched between access point (AP) mode and (ST) Station mode

– Avoid Hard-coding WiFi Credentials.

WiFiManager (ESP8266 WiFi Connection supervisor with fallback web setup entrance) eliminates the need for re-programming the master node if the user updates his WiFi credentials. It will enable the user from entering his WiFi credentials through a configuration dialogue web page, which will be presented as soon as the user connects to the created access point (Master node) through any web browser. As shown In [Figure-6].

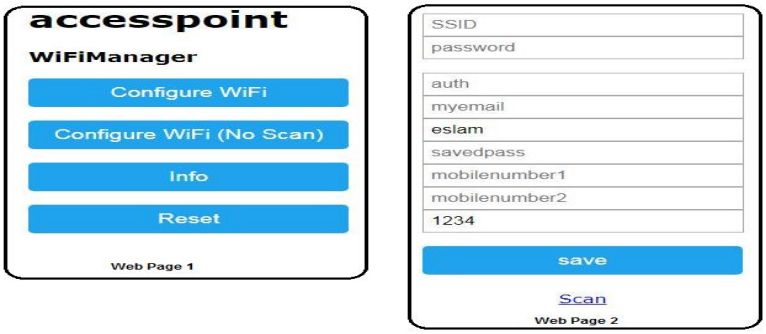

Fig. 6. WiFiManager Configuration Webpage

– Avoid the disappearance of WIFI credentials Configuration after power-off the master node NodeMCU.

Using JSON file to save the configuration data. JSON file used to save & transport a simple data structure.

– Enable the user to do the device configuration Himself, Eliminate the need for professional assistance which saves Money for the user.

Feeding WIFI SSID, Password and Blynk auth token (authorization key) and user email, mobile number and system security password through WiFiManager webpage, use JSON file to save the configuration data.

– Power saving & low power consumption.

Algorithms of deep Sleep Mode protocol for NodeMCU modules are used. Use the sleep functions with the ESP8266 module, make it draw less power and your batteries will last longer. Sensor node only wakes up when an event happened otherwise it's in deep sleep mode. Using temperature sensor LM35 for detecting fire instead of DHT11, because of its low power consumption.

– Connecting the secured building with the owner via two Alternative communication methods.

Both internet and GSM (Global System for Mobile communications) communication methods were used for providing a connection to the building when any of the communication methods fail or temporarily unavailable. Integrate SIM900A GSM module with the master NodeMCU to send a message, dial the pre-configured phone number when

an emergency happened in the secured property.

– Control the security system from any mobile number to ON/OFF or interrogate the State of the system.

Send SMS message from any mobile number formatted as follows:

A. ON+system security password
B. OFF+system security password
C. STATE+system security password

The proposed system security password is configured from the WiFiManager webpage.

– Control the security system remotely through the Internet.

Enable the user to save money of sending an SMS message, effort to control the system manually from the keypad. The Blynk mobile application text input widget enables controlling the system to ON/OFF remotely, by typing:

A. ON+system security password
B. OFF+system security password

– Control the security system manually.

The keypad added an essential feature to the system because it provided the ability to manipulate the security system manually, enable the user from active / deactivate the system or change the system security password. And it is the only way to operate the system manually and stop the alarm in case of the user mobile is out of service for any reason.

– Make a user-friendly interface to the system.

Adding the LCD module to the master node provide visualization option locally to the system shown In [Figure-8], add LCD widget and LED widget in the design of the Blynk mobile application to inform the user remotely about the status of the security system In [Figure-7].

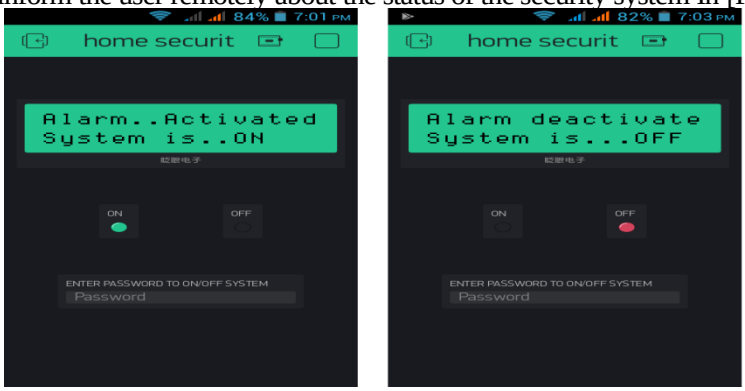

Fig. 7. Blynk mobile application interface

Fig. 8. LCD interface

– The master node can't sense the slave sensor node status message sent to it when it works as station and connected to Blynk cloud to check if the user sends a controlling command from Blynk mobile app, till disconnected from Blynk cloud and work again as an access point to receive slave sensor nodes status.

To solve this problem we make the slave sensor nodes send its status to the master node, wait for the confirmation message from the master node to ensure that the status message of the activated slave sensor node is received by the master node. When the slave sensor node received the confirmation message it goes to deep sleep mode. If the confirmation message from the master node doesn't receive by the slave sensor node then the sensor node will try to send its status again and wait to receive the confirmation message from the master node, it will be wake up till the confirmation message acquired. This solution adds advantage to the system because we don't worry about if there is an unwanted issue in the secured home and the status of its sensor node doesn't receive by the master node due to its busy with something else. That solution makes us sure the sensor node will not sleep until it sends its status to the master node when it is available and receive the status reception confirmation message from the master node.

5.1. Software design

The system software design divided into three parts, the first part is the motion node, door node software design shown In [Figure-9]. And the second part is the gas leakage, fire node software design shown In [Figure-10]. and the third part is the Master node software design shown In [Figure-11]. In the proposed system embedded C-language is used for NodeMCU. Arduino IDE is used for compiling the code.

5.2. Hardware design

The hardware of the proposed security system includes four sections, firstly the Master node consists of NodeMCU module micro-controller, keypad, LCD, led, buzzer and GSM module, that built with Dual-band GSM/GPRS technology based SIM900A modem from SIMCOM. It works on frequencies 900/1800 MHz, Calling a pre-configured number. Sending messages about event detection and receiving control messages are done with the help of AT commands. Microcontroller NodeMCU board is an open source development board and firmware based on the widely used ESP8266 -12E WiFi module used as a central controller. It contains 10 digital pins and 1 analog pin. Secondly, the Motion node consists of NodeMCU IOT module, and Passive Infra-Red (PIR) sensor to detect intrusion based human body infrared rays. If a motion is detected, the sensor will send a signal to the micro-controller. Thirdly The Door node consists of NodeMCU IOT module, reed magnet switch which used to detect a window or door opening. Fourthly the Gas leak, Fire node consists of NodeMCU IOT module, MQ-5 natural Gas Detector Sensor Module, LM35 temperature sensor, buzzer, and relay. The LM35 device draws the only 60uA from the supply, rated to operate over a −55 °C to 150 °C temperature range. The LM35 output voltage is linearly proportional temperature and it's connected to the analog pin of the microcontroller. MQ-5 natural-gas module is suitable for detecting the concentration of LPG, natural gas, town gas in the range of 200-10000ppm. This module provides both digital and analog outputs. Its digital output is connected to the digital pin of the microcontroller where the threshold level for digital output can be easily adjusted using the preset on the board.

5.3. Power consumption

Using deep sleep algorithms with NodeMCU IOT module which wakes up only when an event happened with WiFi RF Disabled. Using static IP address for the node and turn on WiFi module only to send data and then back to sleep mode achieve maximum benefit of saving power consumption and gives the sensor nodes work on battery capability to last longer. The Proposed sensor nodes consume 2.48mA average during deep sleep mode

doesn't exceed 72 mA during other modes of operation. While Semanur KARACA, Ibrahim SAVRUK sensor node draw less than 5mA average and reach 115mA [2]. Table (1) illustrates the power consumption of proposing a sensor node. The time (T) of how long the node will last can be calculated using (1).

$$T = \frac{BV \times BC}{MV \times MA} \tag{1}$$

BV.....Battery Voltage.
BC.....Battery Capacity.
MV.....MCU Voltage.
MA.....MCU Current.

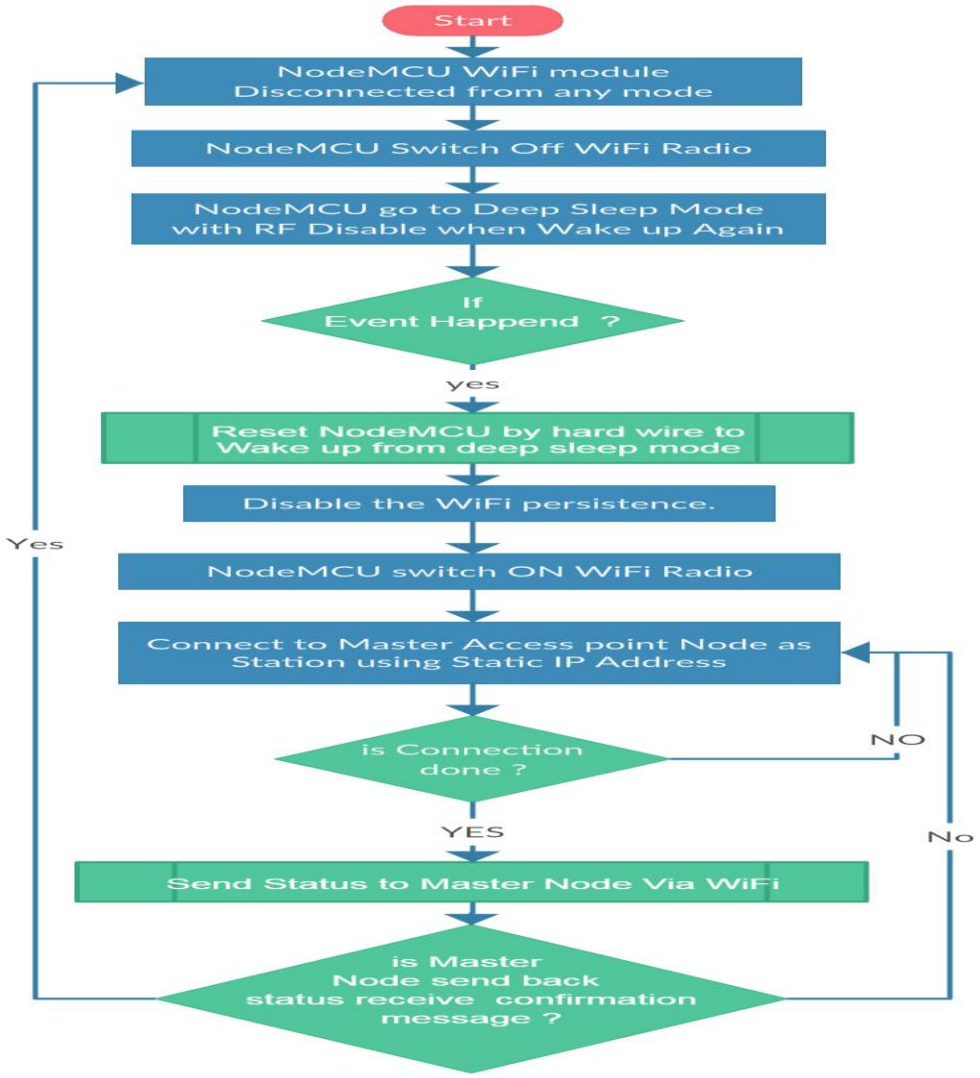

Fig. 9. Motion node, door node software design

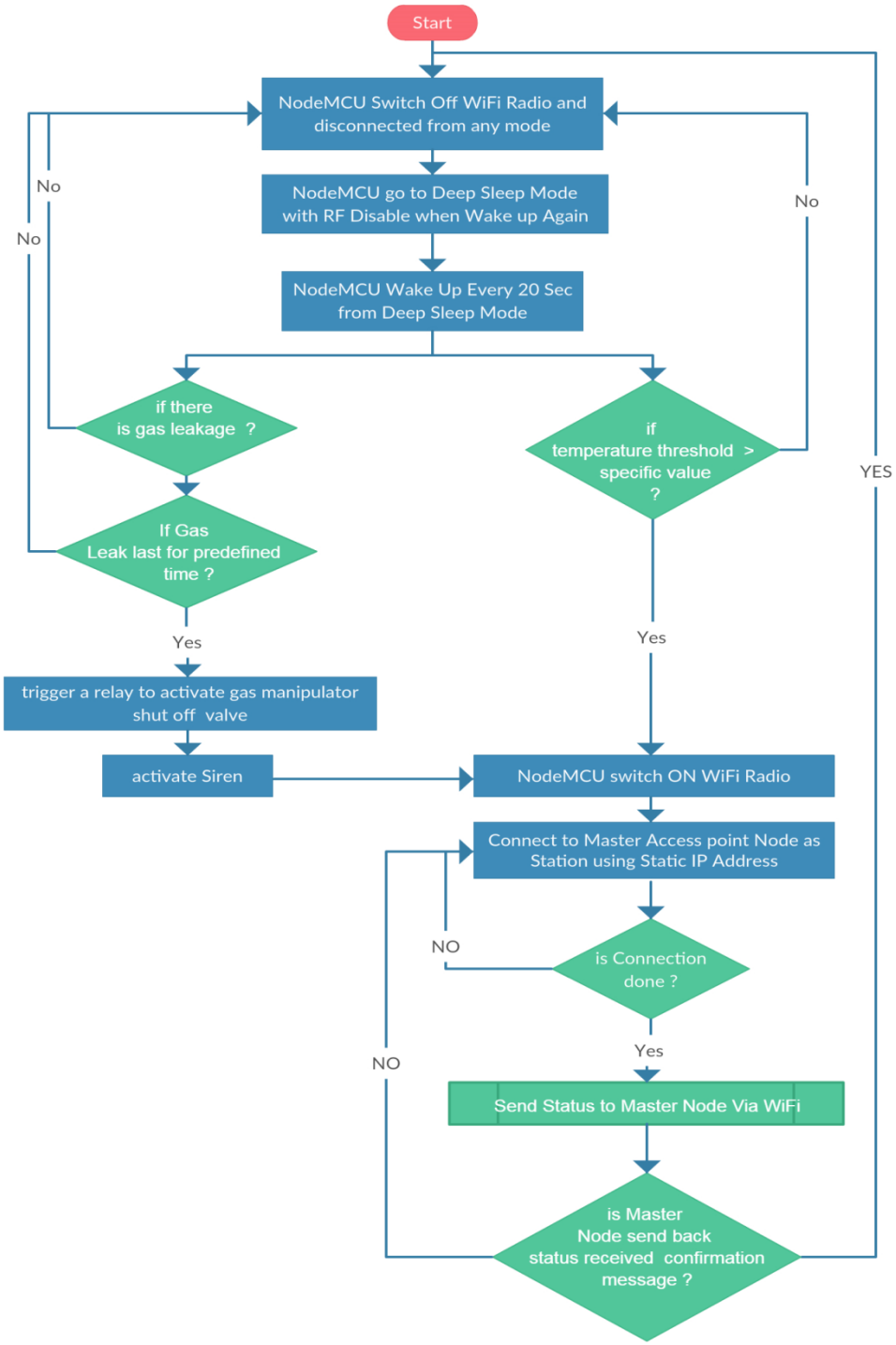

Fig. 10. the gas leakage, fire senor node software design

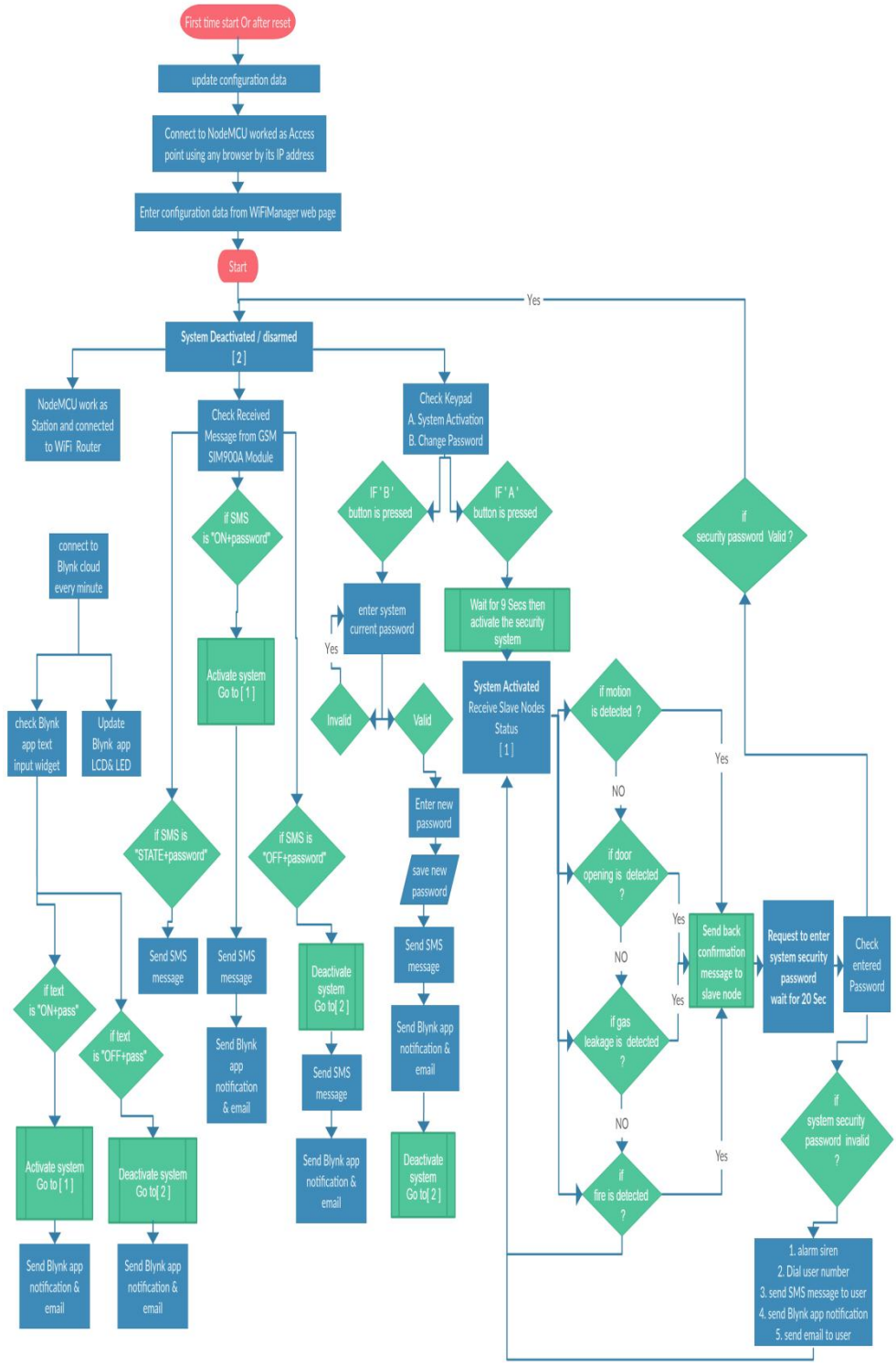

Fig. 11. The Master Control node software design

Table. 1.
Power and Time Consumption of Slave Sensor Node.

Mode of Operation	Power Consumption (mA)		Time Consumption (Sec)	
	Proposed Nodemcu	Normal	Proposed Nodemcu	Normal
Deep Sleep	2.48	0.086		
Wake Up	18.9	210	0.35	0.35
read sensor	18.9	72	1	1
Access point Association	72	74	2.3	2.3
Persisting Connection Information	0	74	0	1.2
DHCP lease	0	74	0	3
Transmit data	72.1	130	0.3	0.3
Total time of operation			3.95	8.15

[Figure-12] has shown the power consumption of the proposed sensor node in different modes. [Figure-13] has shown the time consumption of the proposed sensor node.

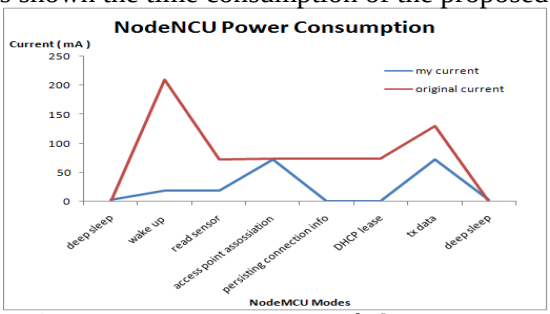

Fig. 12. Power Consumption of Slave Sensor Node

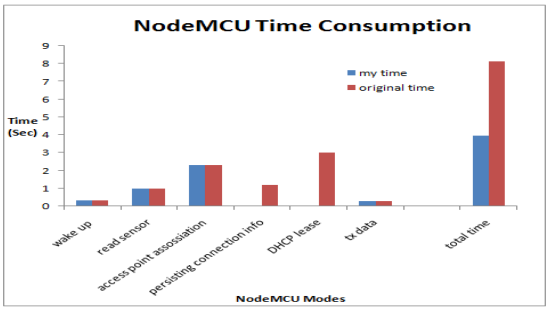

Fig. 13. Power Consumption of Slave Sensor Node

6. Result of implementation

[Figure-14] shows the door sensor node implemented using IoT Module (NodeMCU). The IoT Module is powered based on a normal USB 5V supply. The sensor gets 3.3V supply from MCU and it resets The IoT Module from a deep sleep when the door is open. To wake up from the deep sleep and send sensor status to access point.

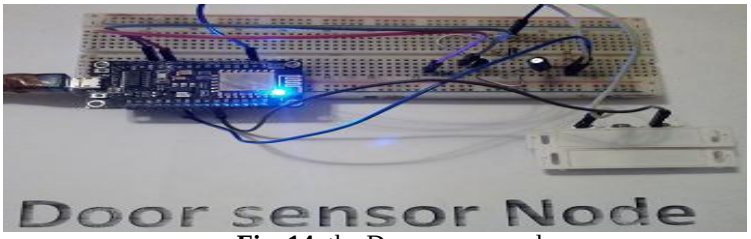

Fig. 14. the Door sensor node

[Figure-15] shows the motion sensor node implemented using IoT module (NodeMCU). The IoT Module is powered based a normal USB 5V supply. The PIR sensor gets 5V supply from MCU and it gives a pulsed output which resets The IoT Module from a deep sleep when there is a motion in its range.

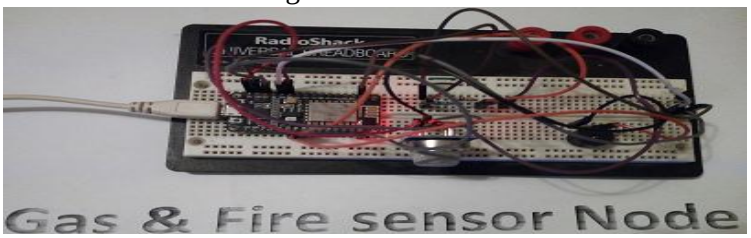

Fig. 15. Motion sensor node

[Figure-16] shows the Gas & Fire sensor node implemented using IoT module (NodeMCU). The IoT Module is powered based a normal USB 5V supply. The MQ-5 gas module gets 5V supply from MCU and it gives digital output to digital pin of NodeMCU using a voltage divider circuit. NodeMCU reads the digital of the sensor and makes a digital pin high to activate a relay which triggers gas shut off valve. The fire sensor LM35 node gets 3.3V supply from the module. The sensor output is connected to the analog pin of NodeMCU.

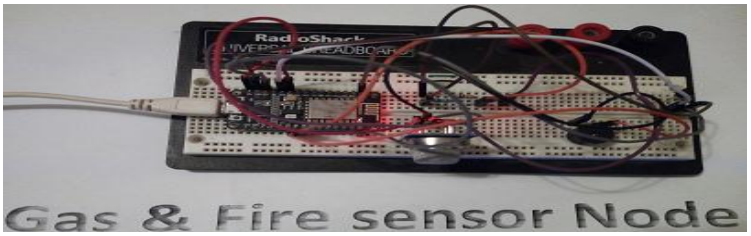

Fig. 16. Gas and Fire sensor node

[Figure-17] shows the Master controller system implemented using IoT module (NodeMCU). It includes a buzzer, GSM Modem, keypad, LCD, led. NodeMCU is powered by USB 5V supply and GSM modem by 5V 2A adapter.

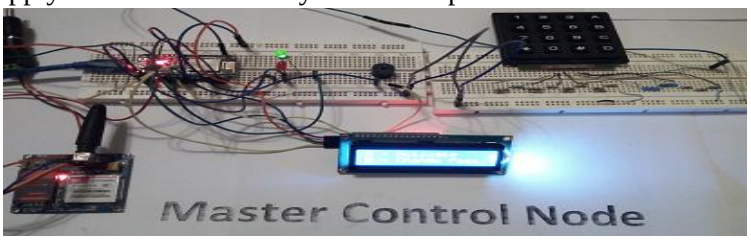

Fig. 17. Master Control Node

The screenshot of the security system mobile application alert notifications are also shown in [Figure-18], the benefit of it is to alert the user remotely using the internet.

[Figure-19-20-21] shows the current consumption in deep sleep, wake up and transmit data modes of door sensor node respectively.

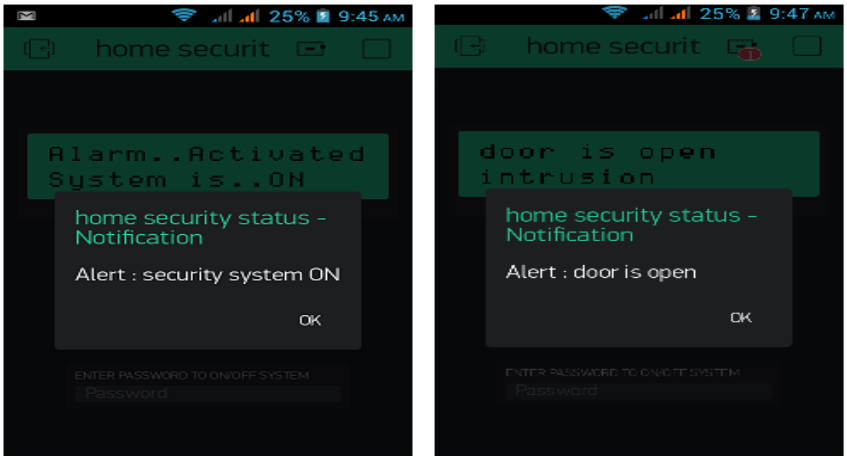

Fig. 18. Blynk mobile application notification

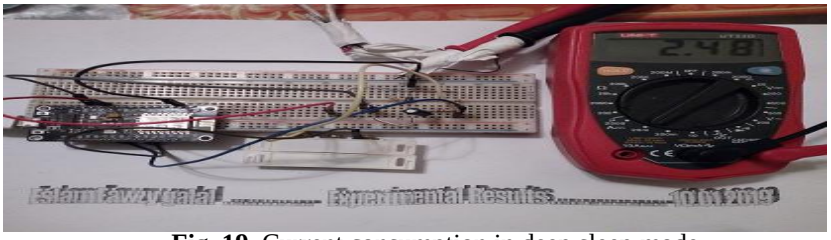

Fig. 19. Current consumption in deep sleep mode

Fig. 20. Current consumption in wakeup mode

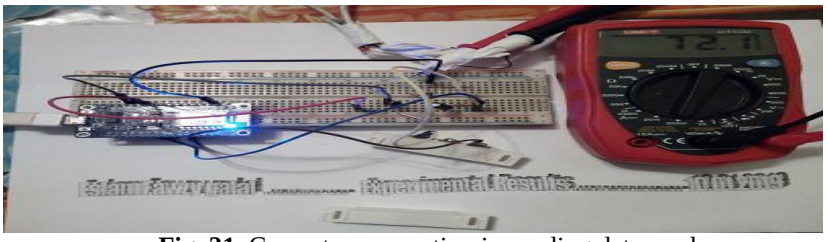

Fig. 21. Current consumption in sending data mode

7. Conclusion

In this paper, we have designed and implemented an economic wireless security system for monitoring using IoT module. The intruder and gas leakage and fire detection are the main features of the system. Using two alternative communication methods internet and GSM to connect the proposed system with the user is an additional advantage of the system. We have used Blynk cloud and Blynk application which helps to alert the user globally with notification, email

when any suspicious event happened. The use of NodeMCU makes the system economic, portable and reliable and scalable. This system is designed with a motive to protect mankind from exposing to burglary, gas leak and fire accidents dangers and with the inspiration of affording economic security system advantages to the common man in the developing countries. The system also equipped with an IP camera that used to Check the secured property when a notification comes to the Owner from the system before taking an action for false alarm Alerts.

REFERENCES

[1] Sruthy S, Sudhish N George, Memeber, " WiFi Enabled Home Security Surveillance System using Raspberry Pi and IoT Module ", 2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)

[2] Semanur KARACA, İbrahim SAVRUK, " A Low Cost Smart Security and Home Automation System Employing an Embedded Server and a Wireless Sensor Network", 2016 International Conference on Consumer Electronics-Berlin

[3] M Akhil Raja, G Rakesh Reddy, Mrs.Ajitha," Design and Implementation of Security System for Smart Home ", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET).

[4] Aadel Howedi, Ali Jwaid," Design and Implementation Prototype of a Smart House System at Low Cost and Multi-Functional", FTC 2016 - Future Technologies Conference 2016, 6-7 December 2016.

[5] Hakar Mohsin Saber, Nawzad Kamaran Al-Salihi, " IoT: Secured and Automated House " 2017 International Carnahan Conference on Security Technology (ICCST).

[6] Md ShariqSuhail, G ViswanathaReddy, G Rambabu, " Multi-functional secured smart home " 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[7] Souveer Gunputh, Anshu Prakash Murdan, Vishwamitra Oree, " Design and Implementation of a Low-Cost Arduino-Based Smart Home System ", 2017 9th IEEE International Conference on Communication Software and Networks.

[8] Ayush Panwar, Anandita Singh, Renu Kumawat, Siddharth Jaidka, Kumkum Garg," Eyrie Smart Home Automation using Internet of Things",Computing Conference 18-20 July 2017 | London, UK.

[9] Mile Mrinal, Lakade Priyanka, Mashayak Saniya , Katkar Poonam ,A.B. Gavali"Smart Home – Automation and Security System Based on Sensing Mechanism"2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT).

[10] Dr. M.L. Ravi Chandra, B. Varun Kumar, B.SureshBabu," IoT Enabled Home With Smart Security", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017).

" نظام أمن المنزل اللاسلكي الاقتصادي بأستخدام وحدة أنترنت الأشياء "

الملخص العربي

تـأمين الانسـان ضـدد التعرض لمخـاطر السرقة وأقتحـام المنـازل وحـوادث تسريب الغـاز والـدخان والحريـق هـو الهـدف الرئيسى لهذا البحث. يوضح هذا البحث تصميم وتنفيذ نظام الأمان القائم على إنترنـت الأشياء فـى المبـانى عن طريـق استخدام متحكم NodeMCU و السحابة الالكترونية Blynk وأتصـال مع شبكة WiFi. يتكون نظام الأمان من شبكة حساسات لاسلكية و وحدة تحكم رئيسية. يعد تنبية المستخدم عن بعد وإمكانية نقل النظام من مكـان لأخـر بسـهولة بواسطة المستخدم وسـهولة تركيبـة وتهيئتة من قبل المستخدم و تـوفير أستهلاك الطاقـة من السمات الرئيسية للنظـام المقترح. حيث تقوم وحدة IOT التـى تعمل بتقنية WiFi بمعالجة البيانات من الحساس المتصل معها وتقوم بأرسال حالة الحساس الـى وحدة التحكم الرئيسية. عند أستقبال إشعار الحدث من الوحدة الفرعية فى شبكة الحساسات, تقوم وحدة التحكم الرئيسية بتنبيـة المستخدم محلياً عن طريـق سـارينة أنذار وعالمياً عن طريق أرسال أشعارات تنبية و بريد الكترونى من خلال السحابة الالكترونيـة Blynk و التطبيق علـى الموبيل Blynk application وكذا الأتصـال برقم موبيل المستخدم وأرسـال رسـائل نصية SMS للهـاتف المحمول عن طريـق شبكة الاتصـالات العالميـة للموبيـل GSM. أستخدام وحـدة أنترنـت الأشـاء IOT NodeMCU فـى أنشـاء كـل عقدة Node بشبكة الحساسات وأيضا فـى أنشـاء وحدة التحكم الرئيسية تجعل النظـام صـغير الحجم, وفعـال من حيث التكلفة وسـهولة الأستخدام. النظام المقترح يقوم بمراقبة المكان المراد تأمينة عن بعد ,وكذا يمكن التحكم في النظام من أى مكان بالعالم.