



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 10, October 2020

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.488

 9940 572 462

 6381 907 438

 ijircce@gmail.com

 www.ijircce.com

Smart Home Security System Using Arduino

Karan Gori , Jay Dudhatra, Tushar Gada, Archana Chaugule

UG Student, Dept. of I.T., Shah And Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

UG Student, Dept. of I.T., Shah And Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

UG Student, Dept. of I.T., Shah And Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

Professor, Dept. of I.T., Shah And Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

ABSTRACT: Internet of Things (IoT) conceptualizes the idea of remotely connecting and monitoring real world objects (things) through the Internet [1]. When it comes to our house, this concept can be aptly incorporated to make it smarter, safer and automated. This IoT project focuses on building a smart wireless home security system which sends alerts to the owner by using Internet in case of any trespass and raises an alarm optionally. Besides, the same can also be utilized for home automation by making use of the same set of sensors. The leverage obtained by preferring this system over the similar kinds of existing systems is that the alerts and the status sent by the Wi-Fi connected microcontroller managed system can be received by the user on his phone from any distance irrespective of whether his mobile phone is connected to the internet. The microcontroller used in the current prototype is the TI-CC3200 Launchpad board which comes with an embedded micro-controller and an onboard Wi-Fi shield making use of which all the electrical appliances inside the home can be controlled and managed.

KEYWORDS: Home Security, IOT, Motion Sensor, Gas sensor, Arduino.

I. INTRODUCTION

Safety and security of any living or working place is one of the most primary concerns. The advancement of the technology has increased the safety and security along with their belongings. Internet of Things (IoT) become major interest as results of technology development and industry revolution

4.0. Application of IoT has been widely implemented in every sector such as security systems, industry, farming, and medicine. Several studies have been developed a IoT-based smart home such as home security system using internet of things. Previous study suggested to use Arduino Uno , module ESP wifi , dan reed sensor, however, in that study only applied sensor reed that placed in front off the door as a security system and users received notification in smartphone after the door opened. This system still has a higher risk for criminalization . Another study, used IoT-

based smart security and home automation system with sensor PIR installed at the entrance of the building, so that if there is a human movement , the sensor will trigger to input the microcontroller, the owner will get a notification through voice calls. This system can provide real action directly for owner to provide warning system by turning on the light and alarm so the owner using the keypad button that has been programmed previous. IoT based smart home using Blynk Framework , this system consists of three different isolated sub-systems including relay module systems, GPS module systems and temperature sensors, as well as PIR sensors and ultrasonic sensors to measure the water level in the connected tank using Nodemcu via Wi-Fi__33, and the interface using Blynk App . Whereas smart home design based on ethernet systems can protect homes and monitor home conditions such as humidity, temperature , gas leak and fire using sensors that are integrated with the Arduino Mega microcontroller and Ethernet shield.

II. LITERATURE REVIEW

Design and Implementation of Security for Smart Home based on GSM technology was discussed by Govinda et al. (2014) that provides two methods to implement home security using IoT. One is using web cameras such that whenever there is any motion detected by the camera, it sounds an alarm and sends a mail to the owner. This method of detecting intrusion is quite good, albeit somewhat expensive due to the cost of the cameras involved in the process. The cam

eras need to be of good quality which means it should have a wide range and the picture quality should be high enough to detect movement. Also if you go for movable cameras such as dome cameras they will cost even more than the fixed ones.

SMS based system using GSM was proposed by Karri and Daniel (2005) propose to use internet services to send messages or alert to the house owner instead of the conventional SMS. Jayashri and Arvind (2013) have implemented a fingerprint based authentication system to unlock a door. This system helps users by only allowing the users whose fingerprint are authorized by the owner of the house. This system can also be used to monitor who all have used the sensor to gained entry into the house. The system is coupled with a few more home protection features such as gas leakage and fire accidents. Although a good system, fingerprint sensors are expensive and complex (as they need increased sensor resolution) to integrate into an IoT setup. Some experts also argue that only relying

on a fingerprint sensor is not wise as it is relatively easy to lift someone's fingerprints and replicate them, which is why it is always advised to use fingerprint scanners in a two factor authentication systems where an additional layer of security is available in the form of PIN, passcode, voice recognition, etc.

Some researchers proposed an idea of robust IoT home security system where a fault in of one component in the system does not lead to the failure of the whole system. The idea of using multiple devices which may or may not be directly compatible with each other but can be made to work in such a way that they can replace an existing component of the system in case of a fault. In tandem to this, the model has the ability to use overlap between various devices which would result in preserving energy thus making the model more efficient. An example provided of the said model would use temperature sensor, WiFi module and a door sensor to replace a faulty camera. The authors are successful in an effort to demonstrate the given example. However such systems are useful for people with energy efficiency in mind and for those who need a high degree of robustness with their security systems and are willing to expend more money than usual.

Laser rays and LDR sensor are used to detect intrusion using their movement was proposed in

2016. The way the system works is that a laser is focused towards a LDR sensor and the moment that the contact of laser to LDR sensor breaks, the alarm connected to the sensor goes off alerting the neighbours and sends a SMS to the owner. This system solves the problem of covering the places which are out of range from the fixed cameras but faces the same difficulties which are faced with systems consisting of GSM modules to send text messages, which is that the delivery of message is dependent

on network coverage. Also due to the nature of lasers being a straight beam, it can be avoided by intruders who know about the system and are capable of dodging the lasers, rendering the whole system useless.

III. ARCHITECTURE

IOT and Arduino Based Home Security System uses four Sensors, namely, Temperature, Smoke, LPG and IR sensors.

Data from these sensors is then sent to the Arduino, which has an inbuilt signal converter. Arduino then sends data over to the Wi-Fi module – ESP8266. ESP8266 is a chip used for connecting micro-controllers to the Wi-Fi network and make TCP/IP connections and send data. Data, which is sensed by these sensors, is then sent to the IOT. To elaborate

on the theft detection, we have connected a password module by which a user can enter the password. The door would open only if the password entered is correct. The IR sensor needs to be installed

on the door, which is, by default activated. If an individual enters the correct password, the IR sensor is deactivated for 10 seconds and the buzzer won't turn ON. If somebody tries to enter the house without entering the password, i.e. by damaging the lock or

so, as soon as the person passes the IR sensor, the buzzer would be turned ON. The buzzer would be turned ON even if a wrong password is entered for consecutively

3 times. To demonstrate the door, we have used a DC motor. The buzzer will turn ON even when it detects incense sticks as well as a candle flame. Temperature and Smoke sensors are used for fire detection. As soon as the fire is detected, the signal will be sent to the micro-controller which will then send appropriate data to the LCD and the Wi-Fi module. Data is in turn sent to the website using the IOT module. Similarly, the LPG sensor is used for LPG gas leakage detection. The Pre-requisite for this project is that the Wi-Fi module should be connected to a Wi-Fi zone or a hotspot. This project is also implemented without the IOT module. In place of the IOT module, we have used a GSM module, by which an SMS is triggered.

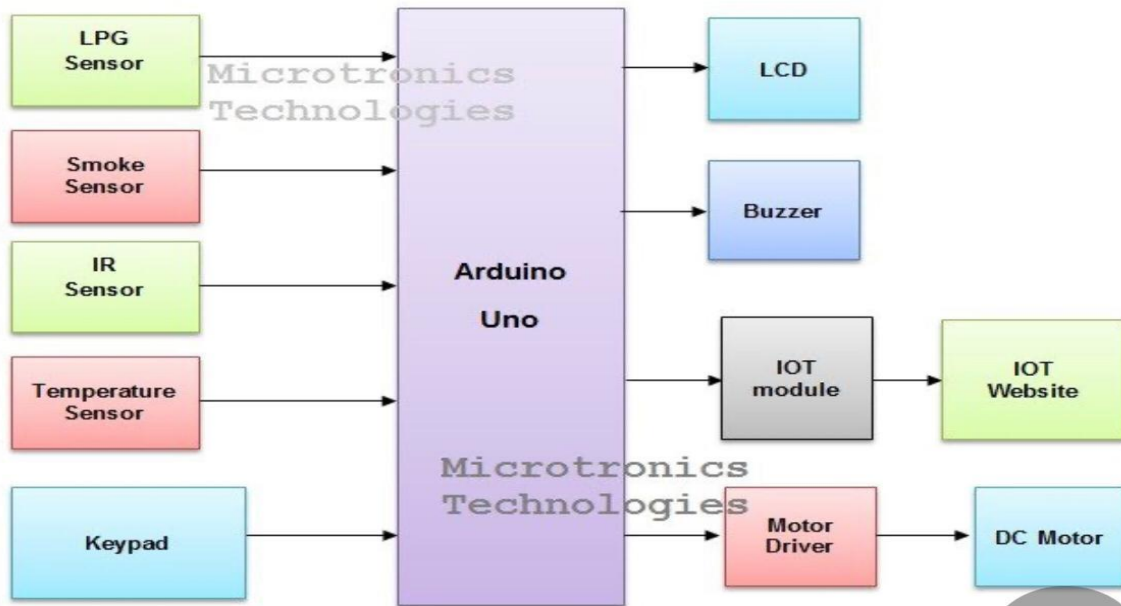


Fig.1. block diagram

IV. WORKING

The smart home promises a futuristic home experience where everything you need is just a simple voice command away, even when you're far from home. There are some very cool gadgets that let you do a lot with home automation, many of which are incorporated into home security systems. These include smart doorbells, smart locks, smart cameras, smart thermostats, smart lights, and smart smoke alarms. One of the most common and security-focused components of a smart security system are smart doorbell cameras. These incorporate a small camera in the doorbell button. When someone rings the bell—or approaches the door, depending on the system—the doorbell sends an alert to your phone and activates the camera, letting you see a clear picture of who's there, no matter where you happen to be. Smart locks are great not only for security but also for convenience, often allowing you to forego keys entirely. What makes them smart is their ability to communicate with your smartphone via Wi-Fi or Bluetooth, allowing you to lock and unlock your door from anywhere. Many also automatically lock and unlock when they detect your phone approaching so that you can come and go without ever having to worry about whether the door is locked. Smart cameras take the traditional security camera concept and turn the dial up to eleven. These cameras incorporate Wi-Fi connections that allow them to be viewed and controlled remotely using a smartphone app. Many can also upload the footage to the Cloud for storage, eliminating the need for a potentially complicated on-site storage setup. The last common home automation feature of a security system is the humble smoke alarm. This device takes the traditional smoke alarm and brings it into the digital age, with Wi-Fi connectivity and the ability to communicate and pinpoint exactly where a fire is located. The really nice thing about these alarms is that they can send the alerts to your phone so you can be aware of any issues even when you're away from home. You can also easily silence them in the event of a false alarm—who hasn't set off their smoke alarms at least once while cooking? Top picks in this category include the Nest Protect and the First Alert Onelink. Both detect carbon monoxide in addition to smoke and alert you in a human voice rather than a screeching alarm tone.

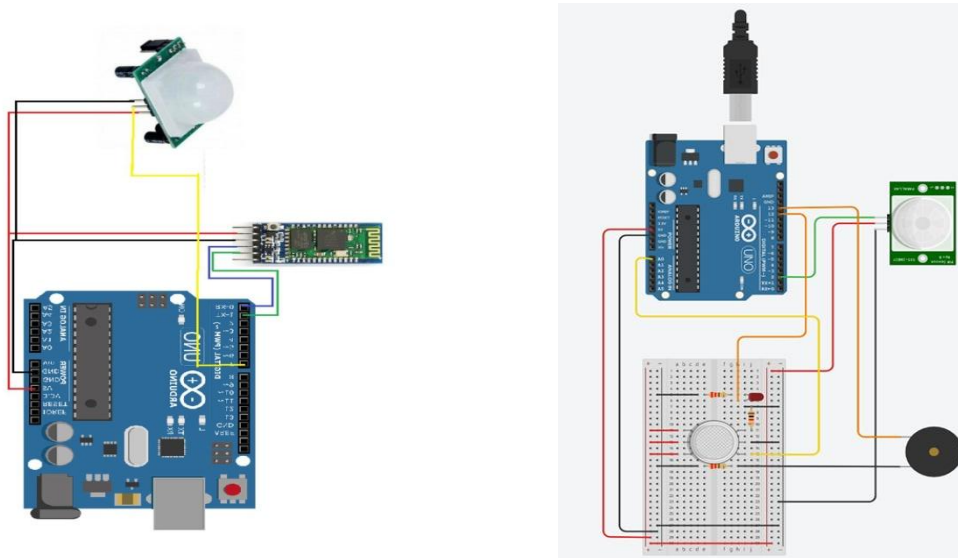


Fig.2. Circuit Diagram

MOTION SENSOR

There is a jumper behind this module. If you move the jumper to L position, the sensor will ‘toggle’ (change state) whenever motion is detected. This is unlikely to be of much use in a practical applications. This mode is called non-triggering or Single Triggering mode.

Moving the jumper to the H position will result in the more usual sensor logic. The sensor will turn on when motion is detected and turn off a while after the last motion is detected. This sensor will reset the timer (which would otherwise turn the output off) each time motion is detected; this would be applicable, for example, for room occupancy lighting control where you don’t want the lights to blink off while the unit resets. This is called Retriggering mode. (or repeatable trigger mode).

There are also two potentiometers behind this module. By changing the SENSITIVITY potentiometer, you can reduce or increase the sensitivity of the sensor (clockwise increase), and also by changing TIME potentiometer the output delay after movement detection will be changed.



Fig.3. Motion sensor

GAS SENSOR

The MQ-2 smoke sensor is sensitive to smoke and to the following flammable gases:

- LPG
- Butane
- Propane
- Methane
- Alcohol
- Hydrogen

The resistance of the sensor is different depending on the type of the gas.

The smoke sensor has a built-in potentiometer that allows you to adjust the sensor sensitivity according to how accurate you want to detect gas.

The voltage that the sensor outputs changes accordingly to the smoke/gas level that exists in the atmosphere. The sensor outputs a voltage that is proportional to the concentration of smoke/gas.

In other words, the relationship between voltage and gas concentration is the following:

- The greater the gas concentration, the greater the output voltage
- The lower the gas concentration, the lower the output voltage

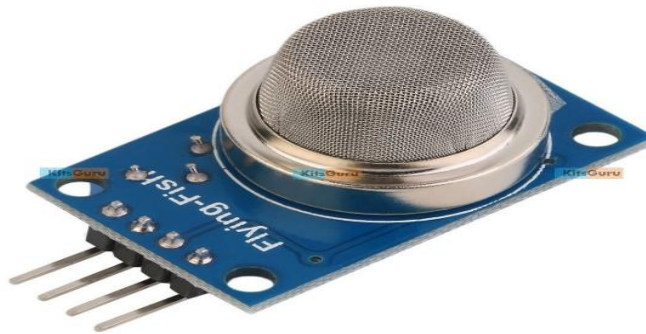


Fig.4. Gas sensor

V. APPLICATION, FEATURES & ADVANTAGES OF SMART HOME SECURITY SYSTEM

Security being the main intent of the project, the most important application of this system is any domestic security. By using this project, a person will be intimidated about any incident likely to be caused by fire, theft, LPG gas – REMOTELY.

This project can be used at Restaurants, Industries, Manufacturing units, Banks, etc.

The main advantage of this system is that it is fully automated. Once installed, it does not require any kind of human interaction. Also, it is very cost-effective.

IOT and Arduino based Home Security System can be enhanced to identify fingerprints as opposed to a password using a keypad.

Additionally, we can have a voice announcement system that would send out vocal instructions regarding any of the hazardous conditions detected by Smoke, Temperature, IR and LPG gas sensors.

VI.OBJECTIVES

The main advantage of this system is that it is fully automated. Once installed, it does not require any kind of human interaction. Also, it is very cost-effective. IOT and Arduino based Home Security System can be enhanced to identify fingerprints as opposed to a password using a keypad.

VII.CONCLUSION

With the advancement in technology, the number of electronic devices in our day-to-day Life has increased to make life simpler. So there is necessity to construct a trustable Remote System that will easily control all these devices from a distance will not only reduce the complexity of handling the number of devices simultaneously, but also save power. This report presents overall design of Home Automation and Security System. This is an IoT based project. After research, we make a successful prototype. Using the Ethernet and microcontroller technology we design a Home Automation System where the entire electrical item will be controlled. Using the internet people can also monitor room temperature, Gas occurrence in kitchen, detect human in room through the user friendly Web Application and also makes a sms notification system. Comparing to others this system is low cost, attractive user friendly interface which is platform independent and it's very easy to install. After implementation of all functions, the system is tested in different stages and it works successfully as a prototype.

REFERENCES

1. Sirsath N. S, Dhole P. S, Mohire N. P, Naik S. C & Ratnaparkhi N.S Department of Computer Engineering, 44, Vidyanagari, Parvati,Pune-411009, India University of Pune, "Home Automation using Cloud Network and Mobile Devices".
2. A. R. Al-Ali and M. AL-Rousan, Java-based Home Automation System, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, May 2004, Meng-Shiuan Pan and Yu-Chee Tseng, "ZigBee Wireless Sensor Networks and Their Applications" Department of Computer Science National Chiao Tung University Hsin-Chu, 30010, Taiwan, 2007.
3. Charith Perera, Student Member, IEEE, Arkady Zaslavsky, Member, IEEE, Peter Christen, and Dimitrios Georgakopoulos, Member, IEEE "Context Aware Computing for The Internet of Things: A Survey". IEEE COMMUNICATIONS SURVEYS & TUTORIAL.
4. Charith Perera_y, Arkady Zaslavskyy, Peter Christen_ and Dimitrios Georgakopoulosy Research School of Computer Science, The Australian National University, Canberra, ACT 0200, Australia yCSIRO ICT Center, Canberra, ACT 2601, Australia "CA4IOT: Context Awareness for Internet of Things".
5. Bill N. Schilit, Norman Adams, and Roy Want, "Context-Aware Computing Applications". Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, a Marimuthu Palaniswamia, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details