LOW-COST AND ENERGY-EFFICIENT SECURITY SYSTEM USING PASSIVE INFRARED SENSOR (IR)

[1]Dhondi Prathibha,[2]Rammohan Togati,[3]Swarnaja Mettu,[4]Gudimala Raju
[1,2,3,4]Assistant Professor
Department of CSE

Kshatriya College of Engineering

***Abstract* — This project introduces a passive Infrared sensor "IR" based security system. We can save power and manage effectively using this sensor at a low cost and with a little amount of memory space. The IR sensor detects changes in infrared radiation levels when an intruder or human passes through the system or location where it is installed. Depending on the change in radiation levels, voltages fluctuate, and with this voltage, the signal is amplified, and therefore sound is created. As a result, it is useful in a variety of applications and fields. When compared to the current system, this type of technology has numerous advantages. The term IR sensor refers to a passive infrared sensor. The primary ideology is one of security. This is based on an IR sensor and an IC that generates a siren or buzzer sound. The IR sensor detects the infrared radiation generated by humans and generates a digital result. It is most commonly found in motion detectors, security alarms, and automatic lighting applications. They detect movement by changing the amount of infrared radiation. This digital output is then sent to the Arduino Uno.**

Keywords— Internet of things, Infrared Communication, Arduino.

I. Introduction

IR motion detectors are one of the most common types of security devices. Passive IR motion detectors are often designed to send an SMS alert to a mobile phone or to an alarm panel in response to detecting IR that indicates the object is moving.

The alarm system isin response to receiving the breach indicator, an alarm condition is triggered. When a human or motor vehicle enters a monitored area, IR motion detectors are typically used in conjunction with indoor or outdoor lighting to switch on a light in response to a person moving in the motion detector's field of view. When someone enters a secure area, an SMS is immediately sent to the corresponding people. People can understand what is going on in the host area. When the owner is in a remote location, they get messages to the host section via SMS and can examine all information about the host section photographs via mobile phone. People can comprehend what is happening in the host location.

When the owner is in a faraway place, they receive SMS messages to the host section and may view all information about the host section images on their mobile phone.

An embedded access control system that is efficient, low in power consumption, and low in cost. Smart home security and remote monitoring based on motion detection are critical for a wide range of commercial and security applications. Many countries are gradually implementing intelligent home security control systems.

Microprocessors are now found in the majority of home and workplace products with which we interact. All of these appliances have some sort of user interface, yet many customers are dissatisfied by the complexity of accessing their equipment' sophisticated functionality.

We are working on a framework that will allow people to interact with appliances using a separate user interface device that they already own.

Since they are generally accessible and have connectivity features that enable them to connect to appliances, smart phones are appealing candidates for delivering interfaces.

Our platform contains an abstract specification language for specifying appliances, a two-way communication protocol, and automatic interface generating software that allows users and the devices they use to be customised [2]. The most significant aspect of any home security system is the ability to detect visitors who enter and exit through the entrance.

II. LITERATURE SURVEY

Cameras must be of high quality. Govinda et al. (2014) explored the Design and Perpetration of Security for Smart Homes grounded on GSM technology, which presents two ways for enforcing home security utilising IOT [1].

One method is to use web cams that detect motion whenever it is detected. When the camera detects motion, it sounds an alarm and sends an email to the owner. Due to the price of the cameras used in the process, this way of detecting infiltration is quite expensive but also very effective. The quality, which implies that it should have a wide range and picture quality that is good enough to detect movement. Furthermore, moveable cameras, such as dome cameras, will cost even more than fixed cameras. Karri and Daniel (2005) presented an SMS-based system employing GSM that uses internet services to send messages or alerts to the house owner instead of traditional SMS. To unlock a door, Jayashri and Arvind (2013) built a fingerprint-based identification system [3].

This method assists users by only permitting users whose fingerprints have been authorised by the house's owner. This method can also be used to track who has used the sensor to gain access to the house. The system is combined with a few other home security functions, such as gas leak detection and fire detection. Although a useful technology, fingerprint sensors are expensive and difficult to integrate into an IoT setup (because to the improved sensor resolution).Some expert also argue that relying solely on a fingerprint sensor is risky because it is relatively easy to lift and replicate someone' fingerprints, which is why fingerprint scanners are always recommended in two factor authentication systems with an additional layer of security available in the form of PIN passcode, voice recognition, and so on. Some researcher offered a proposal for a robust IOT home security system in which a problem in one component of the system does no result in the failure of the entire system [4].

The concept of using numerous devices that may or may not be directly compatible with one another but can be programmed to work in such a way that they can replace an existing component of the system in the event of a fault. In addition, the model has the capacity to employ overlap between multiple devices, which results in energy conservation, making the model more efficient. An example of the abovementioned model would employ a temperature sensor, a Wi-Fi module, and a door sensor. Replace a malfunctioning camera. The authors are successful in their attempt to demonstrate the offered case. However, such systems are beneficial to individuals concerned with energy efficiency and those in need. A high level of robustness in their security systems and are willing to spend more money than usual. The use of laser rays and LDR sensors to detect intrusion based on their movement was proposed in 2016 [5].

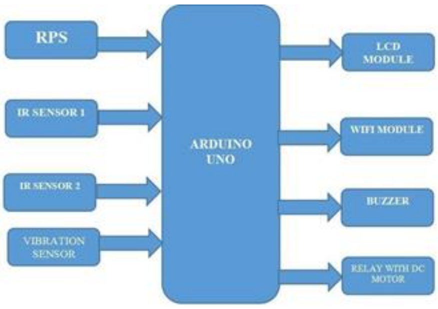
The system operates by directing a laser towards an LDR sensor and measuring the moment it detects it. When the contact between the laser and the LDR sensor fails, the alarm connected to the sensor sounds, alerting the neighbours and sending an SMS to the owner. This approach solves the issue of covering the locations. Which are out of range of stationary cameras but face the same challenges as systems using of GSM modules to send text messages, namely that message delivery is dependent on network availability.

III. PROPOSED SYSTEM

The HC-SR501 Motion Sensor, often known as the IR sensor, is utilised in a variety of Security Alarm and Motion Detector systems. It absorbs infrared signals rather than emitting them, which is why it is known as an IR (Passive Infrared) Sensor. Every item gives off heat in the form of infrared radiation.

As a result, anytime the IR sensor senses a change in temperature, its output pin becomes HIGH. The Pyro electric sensor and Motion Detector IC BISS0001 are the fundamental components of the IR sensor. The BISS0001 IC receives data from the sensor and determines whether theoutput pin is HIGH or LOW.

BLOCK DIAGRAM:



OPERATIONS :

In October 2014, Espressif Systems made a software development kit (SDK) for directly programming the chip accessible, eliminating the need for a second microcontroller..[7] Since then, Espress if has released numerous official SDK updates and still maintains two versions of the SDK: one that is callback-based and the other that is based on Free RTOS. The open-source ESP-Open-SDK[9], which is based on the GNU Compiler Collection (GCC) tool chain and is maintained by Max Filippov, serves as an alternative to Espress if's official SDK.[10] The "Unofficial Development Kit" by Mikhail Grigorev is an additional option.[11][12]

Other, usually open-source SDKs include: Arduino – A firmware built on C++. With this core, it is possible to programme the ESP8266 CPU and its Wi-Fi components just like any other Arduino device. Through GitHub, you may download the ESP8266 Arduino Core.

ESP8266 BASIC is an open-source interpreter similar to BASIC that is designed specifically for the Internet of Things (IoT). a browser-based development environment that is self-hosted.

ESP Easy was created by fans of home automation. ESPHome is a way for your ESP8266/ESP32 using straightforward yet effective configuration files and remotely using home automation technologies.

ESP-Open-RTOS is an open-source ESP8266 software framework that runs on FreeRTOS.

ESP-Open-SDK is an integrated, free and open (to the greatest extent possible) SDK for ESP8266/ESP8285 processors.

Espruino is a firmware and JavaScript SDK that closely resembles Node.js and is constantly maintained. a few MCUs are supported, notably the ESP8266.

ESPurna is open-source firmware for the ESP8285 and ESP8266.

A Lua-based firmware called NodeMCU.

PlatformIO is a cross-platform IDE and unified debugger that is built on top of the libraries and code of Arduino.

Punyforth is a programming language for the ESP8266 that is based on Forth.

Sming is a C/C++ asynchronous framework that is actively being developed. It has excellent performance and numerous network features.

uLisp is a variation of the Lisp programming language createdespecially for computers with little RAM.

ZBasic for ESP8266 — A version of the popular Visual Basic 6 programming language from Microsoft that has been modified as a control language for the ZX microcontroller family and the ESP8266.

Zerynth is an Internet of Things framework for Python programming of the ESP8266[13] and other microcontrollers. Python for embedded devices is implemented in MicroPython, which has been ported to the ESP8266 platform.

An open-source operating system for connected items is called Mongoose OS. ESP32 and ESP8266 are supported. Create in JavaScript or C.[14]

WORKING:

There are many different kinds of infrared-based applications on the market. The transmitter and receiver portions were developed with the circuit for infrared-based applications, thus it cannot be used for other applications. However, the infrared communication project that we completed here may be utilised in any application by just swapping out the application in the infrared LED's location in the infrared communication circuit diagram. We can simply create infrared-based applications utilising this project. The circuit is divided into two sections: the transmitter part and the receiver section.

1. Transmitter portion: The transmitter section comprises of an astable-moded 555 timer IC. The wiring is done as seen in the figure. An IR LED receives its output from astable mode through a resistor, whose working current is constrained. A plastic lens (optics) in the transmitter section of the infrared LED emits IR radiation that is narrowed by the infrared LED.
2. Receiver portion: The silicon phototransistor in the receiver section transforms infrared radiation into an electric current. It ignores slowly varying infrared radiation from ambient light and only reacts to the transmitter's quickly pulsating signal. An infrared receiver module and a led indicator are both part of the receiver section. Depending on the value of the RC combination, the IR Led turns off after a few seconds when the signals are lost.Simply by putting the lens between the IR transmitter and receiver, we may increase the distance between them. We can get the output by supplying a 6V power source to the circuit after connecting the IR transmitter and receiver circuit. This circuit is very easy to utilise in any application.

3. For instance, if an IR circuit's output is connected to a buzzer circuit, the buzzer will make noise when the signals are cut off. A single bread board or PCB can accommodate the mounting of both the transmitter and reception components. To prevent misleading indication owing to infrared leakage, the infrared receiver must be positioned behind the IR LED. The IR rays released by the IR Led are actually reflected by a nearby moving object.

IV. CONCLUSION

The development of wireless and embedded technology resulted in the creation of the "THE IOT BASED HOME SECURITY SYSTEM," an efficient safety and security system. Since everything is connected, it is possible to track at any time and from any location. It can be said that every aspect of this project has been completed satisfactorily, even though there are still some flaws. However, as the adage goes, flaws are only ideal from a beautiful vantage point.

The sensors in this home security system may be controlled and the user can receive updates on them thanks to its low-cost construction and readily available components. To create a smart home system that can instantly update the data that users receive from all sensors and devices. Any house or workplace area may readily alter this system. The designed home security system was put through a number of tests and was able to successfully control the various home security sensors.

Finally, this home security system may still be used to control a range of home appliances while being deployed using Bluetooth, Infrared, and WIFI communication. As a result, this system is adaptable and scalable. to create a smart home system that may make a user's life safer, more comfortable, and convenient. he user may undoubtedly live a safe, comfortable, and convenient life with the help of a smart home system by combining the three primary functions of security, monitoring, and one system. Additionally, there are various problems and difficulties that emerge after completing this project two. The correct wiring of every wire is the first problem. Due to the large number of sensors or devices that require wire connections, everything is connected so haphazardly, which makes troubleshooting more challenging.

FUTURE SCOPE :

The smart home system can be improved in the future by incorporating artificial intelligence techniques, such as the ability to handle domestic emergencies automatically. For instance, the system can assess the seriousness of specific situations by automatically reporting to the police station and informing the user of a theft intrusion.

Additionally, CCTV can be incorporated to the system to increase the project's security component. We have a broad scope to develop in this project and work on it.We attempt to highlight a few tasks that will be introduced in the future. Utilising image processing, incorporate a particular camera, and try to identify both known and unknown faces. If a recognised face is detected, the system can send an email and SMS with a picture and any previously stored data about the face. We can improve user friendliness for the online application. Technology for voice instructions is addable.

REFERENCE :

[1] Andrea Z and Lorenzo V., “Internet of Things for Smart Cities,” IEEE Internet of Things Journal, vol/issue: 1(1), Feb 2014.

[2] Isna K. and S. D. Sawant, “Integration of Cloud Computing and Internet of Things,” International Journal of Advanced Research in Computer and Communication Engineering, vol/issue: 5(4), Apr 2016.

[3] Sonali D. T., “Cloud Computing and Software-Based Internet of Things,” International Journal of Advanced Research in Computer Science and Software Engineering, vol/issue: 6(4), Apr 2014.

[4] Jonathan K., “Using Active Queue Management to Assist IOT Application Flows in Home Broad band Networks,” 2017 IEEE Internet of Things Journal, vol/issue: 4(5), Oct 2017.

[5] Pengfie Z., et al., “Secure Location of Things(SLOT) : Mitigating Local Spoofing Attacks in Internet of Things,” IEEE Internet of Things Journal, vol. 4, Dec 2017.

[6] Akriti S., et al., “Intelligent Accident Management System using IoT and Cloud Computing,” 2nd International Conference on Next Generation Computing Technologies, Oct 2016.

[7] C. Chatrapathi and N. R. Venkatesakumar, “VANET based Integrated Framework for Smart Accident Management System,” International Conference on Soft- Computing and Network Security, Feb 2015.

[8] Priyal R. and Vanthana S., “Car Accident Notification System based on Internet of Things,” International Journal of Computer Applications, vol/issue: 107(17), Dec 2014.

[9] H. M. Ali and Z. S. Alwan, “Car Accident Detection and Notification System Using Smartphone,” International Journal of Computer Science and Mobile Computing, vol/issue: 4(4), pp. 620-635, Apr 2015.