HOME SECURITY SYSTEM USING ARDINO WITH IOT

Md Ami Sohel
Department of ECE
Lords Institute of Engineering and Technology Hyderabad, India

Mohammed Abdul Salman Bari
Department of ECE
Lords Institute of Engineering and Technology Hyderabad, India

HAMAD BIN KHALED
Department of ECE
Lords Institute of Engineering and Technology Hyderabad, India

MOHAMMED ABDUL RAHMAN
Department of ECE
Lords Institute of Engineering and Technology Hyderabad, India

Mr. Dr. Altaf C
Assistant Professor
Department of ECE
Lords Institute of Engineering and Technology Hyderabad, India

ABSTRACT

Westernization of today's society has led to the increase in the number of small families while the gradual spread of living into the suburban areas has raised a significant concern in the security of the individuals. Although there are many security systems available in the market today, they are mostly expensive. The objective of the model described in this paper is to present a simple and low-cost design to make our homes smarter and safer. The Adriano based framework built in this project comprises of PIR sensor, IR sensor, piezoelectric sensor and Sound sensor which not only alerts an intruder action but also captures the images and recordings through a camera from the scene. An intrusion can be identified with the help of the above mentioned sensors that can detect the presence of a person, temperature variations and sound at the location. In case of a deviant output from the above measurements, the owner of the house is immediately alerted through IOT. The rightful person receives a message on his phone immediately followed by images of the person causing the skeptical situation along with a captured video that gives a detailed picture of the happenings and will also serve as an evidence for further investigations.

I. INTRODUCTION

IoT or Internet Things refers to the network of connected physical objects that can communicate and exchange data among themselves without the need of any human intervention. It has been formally defined as an “Infrastructure of Information Society”, because

*e*ISSN 1303-5150

IoT allows us to collect information from all kind of mediums such as humans, animals, vehicles, kitchen appliances. Thus any object in the physical world which can be provided with an IP address to enable data transmission over a network can be made part of IoT system by embedding them with electronic hardware such as sensors, software and networking gear. IoT is different than Internet as in a way it transcends Internet connectivity by enabling everyday objects that uses embedded circuits to interact and communicate with each other utilizing the current Internet infrastructure.

The term IoT and its conception can be traced back to 1985 when Peter T Lewis spoke about the concept during his speech at Federal Communications Commission (FCC). Since then the scope of IoT has grown tremendously as currently it consists of more than 12 billion connected devices and according to the experts it will increase to 50 billion by the end of 2020. The IoT infrastructure has helped by providing real time information gathering and analysis using accurate sensors and seamless connectivity, which help in making efficient decisions. With the advent of IoT both manufacturers and consumers have benefited. Manufacturers have gained insight into how their products are used and how they perform out in the real world and increase their revenues by providing value added services which enhances and elongates the lifecycle of their products or services. Consumers on the other hand have the ability to integrate and control more than one devices for a more customized and improved user experience.

An important factor to consider when we talk about home automation is Security. Home security is a very important feature of home automation and maybe the most crucial one. Home security made a drastic changes in the past few decades and continue to advance much more in the coming years. Previously home security systems meant having an alarm that would go off when somebody would break in but a smart secure home can do much more than that. Therefore the main objective of our work is to design a system which can alert the owner and others of an intruder break-in by sending a notification to their smart phones. The owner will also have the ability to stop or start the alarm remotely using just his smart phone. This system will help the users to safeguard their homes by placing the system on the doors or windows and monitoring the activity through their smart phones.

There has been an unprecedented growth in the number of devices being connected to the Internet since past few years. All these devices connected to the internet are part of the IoT infrastructure which can that allows these devices to send and receive data among each other. This is why it is beneficial to use such an existing infrastructure for designing the proposed security system. An alarm system that sounds the buzzer is of no use when a user is not present in the home to take action. When the owner is away communicate with each other. The IoT network consists of embedded electronics, sensors and software from their home, they want to be assured that their home is protected by intruders and thieves while they are gone. This is why the proposed system keeps the owner informed in the real time about the security status of their home. The designed system informs the user as there is a break-in so that the user can take necessary actions.

The paper is organized as follows: Section 1 discuss about the introduction of IOT and its applications. Section 2, gives a details review of the focus of the paper. Section 3 talks about the materials and the

*e*ISSN 1303-5150

methods to implement the proposed systems. Section 4 proposed the working model of the proposed system, whereas section 5 gives the configuration of the application. Section 6 explains the experimental results followed by conclusion and future enhancement as Section 7.

II. LITERATURE SURVEY

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 [1]. 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 cameras 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.[2] Jayashri and Arvind (2013) have implemented a fingerprint based authentication system to unlock a door [3]. 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 [4]. 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 to detect intrusion using their movement was proposed in 2016 [5]. The way the system works is that a laser is focused towards a LDR

*e*ISSN 1303-5150

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.

www.neuroquantology.com

***e*ISSN** 1303-5150

between 2014 and 2015, drone sales increased 63% and have only continued to rise. However, like all sorts of technology, drones are not flawless. In addition, if you are a drone owner, it is vital to remember possible issues you will encounter. So let us explore a couple of common drone problems and the way to repair them.

In this paper the author says, "Force and torque were used as control variables in a mathematical model". Finally, a nonlinear optimal control problem was used to assess the hex copter's mobility, showing the difficulties in moving the x and y coordinate directions due to the lack of actuators on those axes. Position control for a hex copter was designed in this paper. An extra controller was added to reject the modelling error.The most common approach is to use the Failure Detection and Isolation (FDI) filter and then reconfigure the controller, but the FDI is too complicated for the hex copter, so the controller was modified to use the Modified Linear Extended State Observer (LESO), which does not use the failure detection or reconfiguration strategy. The controller managed a safe flight, but there are still improvements to be made in terms of performance during the flight.

According to author, "the compression of a low volume aerosol in an unmanned octocopter is possible. The octocopter's primary rotor measures 3 meters in diameter and can carry a payload of 22.7 kilograms. Every 45 minutes, at least a gallon of gasoline was consumed. This research cleared the door for the development of aeronautical application systems for drones, allowing for the production of products with greater target speeds and larger Volume Median Diameter (VMD) droplets. According to author, "an octocopter has 6 BLDC motors and 2Lipo batteries with 6 cells and 8000 mAh capacity". Their research also includes measuring the size and density of the droplets, as well as the spray rate and pressure of the spray fluid. They succeeded in developing a drone that can deliver 5.5 liters of liquid with a 16-minute resistance using their project.

The authors observed that to make an octocopter drone and its spray mechanism, one would need some basic and affordable equipment. The universal spray system is used to spray liquid and solid substances. In their investigation, they looked at a variety of agricultural controllers and concluded that the octocopter system with the Atmega644PA is the most suitable due to its efficient implementation. The usage of UAV is not new; it has been in production since the early 1900s. The technology was initially driven by military applications in World War I and expanded by World War II. Military UAV applications are more advanced than civilian

*e*ISSN 1303-5150

applications. The civilian applications are likewise evolving in the same directions, due to their rapid utilization in various applications such as firefighting assistance, police observations of civil disturbances and scenes of crimes, reconnaissance for natural disaster response, border security, traffic surveillance and precision agriculture.The authors utilize unmanned UAVs equipped with cameras for site-specific vineyard management. Normalized Differential Vegetation Index (NDVI) values acquired by the Tetracam ADC-lite camera mounted on VIPtero were compared to ground-based NDVI values measured with the FieldSpec Pro spectroradiometer to verify the precision of the ADC system. The vegetation indices obtained from UAV images are in excellent agreement with those acquired with a ground-based high-resolution spectroradiometer. The work in this journal addressed the design of an autonomous unmanned helicopter system for remote sensing missions in unknown environments. Focuses on the dependable autonomous capabilities in operations related to Beyond Visual Range (BVR) without a backup pilot by providing flight services. Utilizes a method called Laser Imaging Detection and Ranging (LIDAR) for object detection, which is applicable in real-world development.

differential GPS. Navigation systems based on vision regularly choose between a single or stereo camera. Stereo vision lends itself to estimating the distance of features from the cameras via observation, whereas single-camera systems need other distance sensors such as ultrasound. If the drone's compass is not calibrated properly, drone users may experience the flight direction being wrong or abnormal during flight. This can also occur if the drone is fitted with a mounted flight controller and therefore the specifications are simply misplaced. This is why it is vital to offer your drone a quick inspection before each flight. Calibrating the compass can usually help solve this issue but sometimes a restart of the remote control can help. If none of those solutions work, then drone repair services could also be needed to detect the basis of those drone problems.

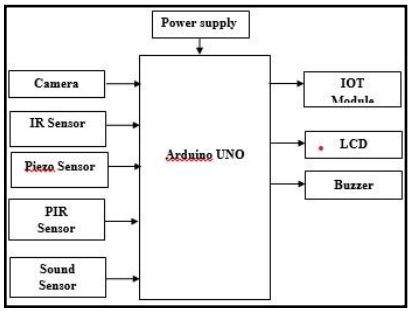
Generally, all aircraft are equipped with an IMU (inertial measurement unit), which is nothing more than a device that incorporates information from accelerometers, g
GPS drift is a problem that may be overcome by combining data from an IMU or by employing a

eISSN 1303-5150

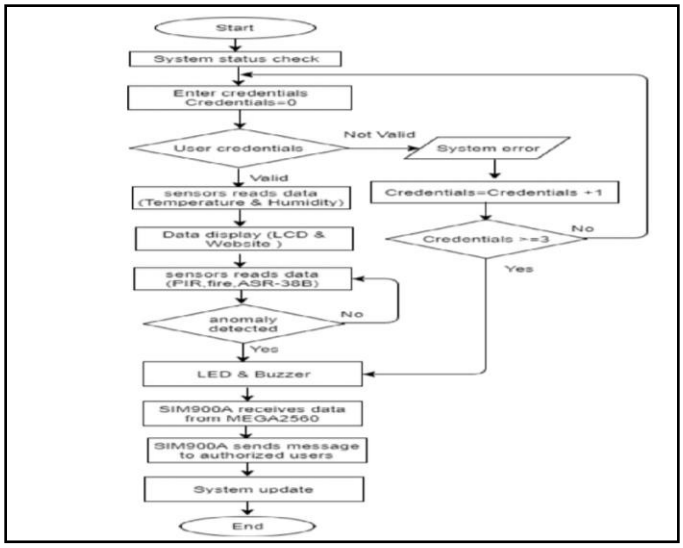
III. SPECIFICATIONS

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 de-activated 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 O

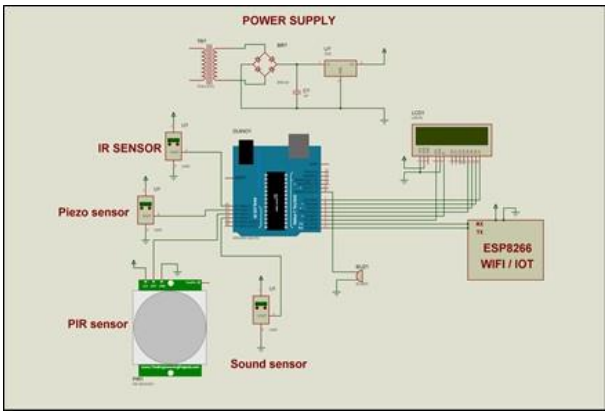
IV. BLOCK DIAGRAM



VI. FLOW CHART



eISSN 1303-5150



VII. Schematic Diagram

VIII. WORKING MODEL

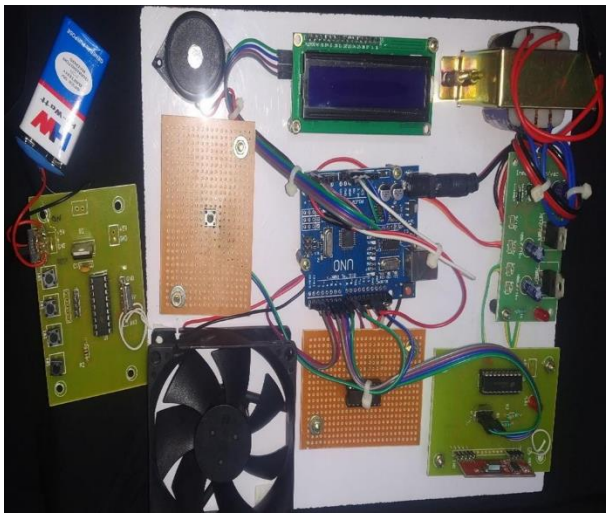


Fig: Working Model

IX. CONCLUSION

The sensors placed on the door informs the home owner as soon as the door is opened by sending a Push notification. The user will get this notification irrespective of whether the phone is locked or unlocked or even if any other app is opened at the moment. This was the main objective of the project, which is the user feels safe and not worry about any intrusion or break-ins when he is away from home. This setup can also be used in commercial offices where some areas are restricted for certain personnel, such a system will immediately inform the administrator of any unauthorized personnel trying to access such an area. Therefore the extensibility and applicability of such a system is only limited only by the imagination. Another important component of the project is the connectivity between the ESP8266 (WiFi module) and the Blynk server. The system successfully connected to the Blynk server using the authentication token and the Blynk libraries. As a result, we were able to get the notification on our smart phones as soon as there was any change in the status of the reed module sensor. Also the additional ability to control the alarm remotely is very beneficial and can be very useful in some unforeseen circumstances. It was also observed that the Blynk app worked smoothly and carried out all communication between the hardware and the app very accurately.

X. FUTURE SCOPE

The developed system can also be used to in industrial and commercial applications such as offices, warehouses and other areas where some areas are reserved for authorized personnel only or other places where safety and precautions are of primary concerns such as internet server room of a big MNC from where corporate data can be stolen. The system can also be easily upgraded to add extra safety features such as cameras, motion detection sensors, etc. for increased safety. The system can also further be developed by adding an RFID scanner so that the authorized users need only carry a RFID or NFC tag with them on their person. The RFID scanner will work by scanning the tag wirelessly and if the user is authorized to enter, the alarm system will

*e*ISSN 1303-5150

be disabled for some time so that the user can enter

XI. REFERENCE

[1] America's Climate Choices: Panel on Advancing the Science of Climate Change; National Research Council (2010). Advancing the Science of Climate Change. Washington, D.C. The National Academies Press. ISBN 0-309-14588-0.

[2] Aviation Safety Unmanned Aircraft Programmed Office, in McBride Paul. Beyond Orwell: the application of unmanned aircraft systems in domestic surveillance operations (2009).Journal of Air Law and Commerce Summer Vol. 74, No. 3, pp.627-628. [3]Bolkcom, C. (2004), Homeland security: unmanned aerial vehicles and border surveillance. Congressional research service reportfor Congress.

[4]USAir force (2010), "MQ-9 Reaper", available at: http://www.af.mil/AboutUs/FactSheets/ Display/tabid/224/Article/1 04470/mq-9-reaper.aspx (accessed: 15 August 2014).

[5]http://www.agx.com.br/n2/pages/index.php , (accessed: 15 August 2014).

[6] Herakovic, N., Simic, M., Trdic, F. and Skvarc, J.(2011), "A machine-vision system for automated quality control of welded rings," Machine vision and applications, vol. 22, no. 6, str. 967- 981, doi: 10.1007/s00138-010-0293-9.

[7]http://www.amazon.com/b?node=8037720 011, (accessed: 15 August 2014).

[8] Meng Leong, B.T., Low, S.M. and Po-LeenOoi, M. (2012), "Low- Cost Microcontroller-based Hover Control Design of a Hexacopter", Procedia Engineering, Vol. 41, pp. 458 – 464

[9] Bresciani, T. (2008), "Modeling, Identification and Control of a Hexarotor Helicopter", master's thesis, Department of Automatic Control, Lund University, Sweden.

[10] Erginer, B. and Altug, E. (2007), "Modeling and PD Control of a Hexarotor VTOL Vehicle," IEEE Intelligent Vehicles Symposium, pp.894-899.

[11] Tayebi, A. and McGilvray, S. (2006), "Attitude stabilization of a VTOL Hexarotor aircraft," IEEE Transactions on Control Systems Technology, vol.14, no.3, pp. 562- 571.

[12] Nonami, K., Kendoul, F., Suzuki, S., Wang, W. and Nakazawa, D. (2010), "Autonomous Flying Robots – Unmanned Aerial Vehicles and Micro Aerial Vehicles", Tokyo: Springer, pp.48-52. 48 Ostojić et al. IJIEM

[13] Heong Ang, K., Chong, G. and Yun Li (2005), "PID control system analysis, design, and technology," IEEE Transactions on Control Systems Technology, vol.13, no.4, pp. 559- 576.

*e*ISSN 1303-5150

***e*ISSN** 1303-5150