International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

DESIGN AND IMPLEMENTATION OF IoT BASED INTELLIGENT SECURITY SYSTEM

Aishwarya B[1], Bindu S M[2], Molugu Surya Virat[3],Manjunath R Kounte[4]

[1,2,3,4] *School of Electronics and Communication Engineering,*
REVA University, Bengaluru-560064 (India)

ABSTRACT

The deployment of IoT on smart systems is based on ease of every user in accessing and controlling the system remotely with the help of internet. By using IoT technology in case of smart home, users can access and control all devices in the home anytime and anywhere through mobile devices as long as the mobile devices are connected to the internet. An efficient, low power consumption and low cost embedded control system for smart security and remote monitoring based on motion detection is very important for wide range of commercial and security application. It is necessary to develop a framework that allows users to interact with appliances through a separate user interface device that they are already carrying. Smart phones are best candidates for providing interfaces because they are widely used in common, have communication capabilities to allow connection to devices, and are already being used for a wide range of different applications. Hence, this paper presents an interesting IoT based security alert system, in which the system detects the presence of an intruder and sends an Email containing the pictures of an intruder as an attachment with date and time, which are captured and is triggered by raspberry pi. Raspberry Pi is used to control the whole system. This design system also quickly alerts user by sending him an alert through GSM module either by SMS or a call to check the mail.

Keywords: *Email alert, IoT, MIME, Raspberry Pi 3, and Security.*

I. INTRODUCTION

In the early years, before the advent of Internet of things (IoT) the everyday individual computations, calculation of data and tasks were handled by the calculators, PC, laptops etc. but the communication was carried out separately by faxing, paging, mailing etc. Whereas, the evolution of IoT brought the idea of exchanging the data by remotely monitoring, accessing, connecting, computing and communication of real world physical and virtual objects through internet. IoT overcomes the disadvantage of Limited range of communication and controlling the networked real world physical objects when compared to technologies like Bluetooth, GSM, and GPRS etc. IoT is an ecosystem of wide range of network area, in which various physical objects are connected to a common network path by providing communication and exchange of data with one another and can also control each other through internet. The path which is being networked can be either an embedded hardware, software or a sensor and also provides Data and Security management. The IoT can be mapped to a Ubiquitous computing as it connects the people and objects and also enables computing from anything, anyone, anywhere and anytime. IoT can be used in variety of applications like Smart Home, Smart

City, and Smart Grid etc [1]. Hence, IoT is expected to generate large amount of data from diverse locations, with consequent necessity for quick aggregation of data, and an increase in need to index, store, and process such data more effectively. Due to the advancement in IoT technology, the communication is made easier by enabling smart devices and also making them safer and automated [2].

Security is a challenging and a progressing domain of research in the recent trends. Security plays a major and key important role in device, data and network protection from the intruders, by designing the effective and efficient protocols and technologies to maintain the data integrity and also for monitoring and controlling of unauthorized access of data.Network security provides an authority to access and control the data in a network and safeguards network resources by a unique name and a password, which effectively limits unauthorized access, but adds a disadvantage of not recognizing the corrupted data being sent over the network. IoT security is a field of venture and an emerging area concerned with protecting the associated connected devices (objects) and networks in Internet of things. Security has a potential risk of large number of unsecured devices connecting to the Internet [3].

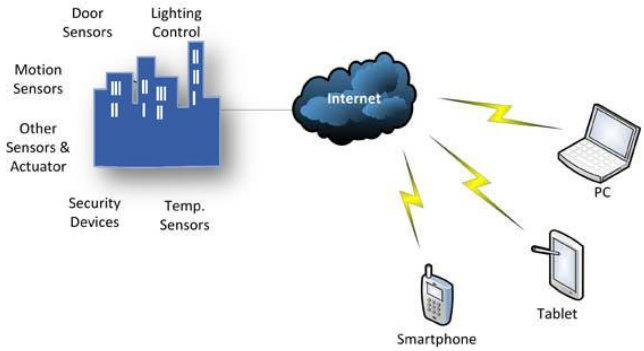

Figure1: An Overview of IoT System.

In the world of Internet of Things, when we have all the technologies to revolutionize our life, it is a great idea to develop a security system which can be monitored and controlled from anywhere by an authorized user. The subsequent sections of this paper are organized in a flow and is as follows: the comparative analysis and literature survey of the similar existing projects are described in the Section 2, the proposed work and design features of hardware and software requirements with their description are described in Section 3, the flow of system implementation and methodology is described in Section 4, the system result is described in Section 5, and Some further modifications which can be done to increase the fidelity and user friendliness of the current prototype with conclusion have been discussed in Section 6.

II. LITERATURE SURVEY

In this section, we present the survey and analysis of few similar earlier research paper contributions from national and international journals in the same domain.

Ravi Kishore Kodali et.al [4], describes that Internet of Things (IoT) visualizes the idea of remotely connecting and monitoring real world objects/things through the internet. In this paper, the advantage of preferring the proposed 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 proposed prototype of the system sends an alert to the authorized user over the calls using internet if any sort of human movement is sensed near the entrance of his house and also alarms upon the user's choice. On the other hand, if the owner identifies that the person is an unexpected guest, then instead of triggering the security alarm, the user/owner can make arrangements such as opening the door, switching on various appliances inside the house, which are also connected and controlled by the microcontroller in the system. The entire system is controlled using the TICC3200 Launchpad.

Shaik Anwar et.al [5], describes the implementation and deployment of wireless control system and accessibility in a home environment for authenticated people only. A PIR motion sensor and camera module are used to detect motion and capture images respectively, makes the security system alive as per the request. Additionally, voice alert or siren is activated to alert neighbors when intruder will be detected. The system identifies the visitor's presence, capture and transfers the image through email automatically to home owner. The system also generates voice output whenever a person tries to enter into the house. The user can directly login and interact with the embedded device in real time without the need to maintain an additional server. This paper presents the design and the implementation of an interactive Smart home security system with Email alert, Web enabled video streaming and remote control of Voice alert and Door accessing system using Smart Phone. The smart mobile phone based monitor and automatic control of equipment is forming a trend in automation field. Replacing PC with low-cost single chip processor which can make administrators to get parameters of different remote devices and send control information to field equipment at any time through Internet.

III. PROPOSED WORK AND SYSTEM DESCRIPTION

According to the analysis of various common researches, the IoT based security alert systems are designed in such a way to alert the user based on the motion detection of an intruder which is sensed by a PIR sensor deployed at the entrance of the system which when detected, triggers the Raspberry Pi to command the PI camera to capture the picture at the moment of the intruder detection. The images so captured by the PI camera are saved in the SD card or an USB pendrive which is inserted or connected to the Raspberry Pi and are sent as an attachment to the user's registered mail ID with the date and time of the image capture as the name of the picture. The entire design system works smoothly only when the system is connected to a Wi-Fi network or has an internet connection. The limitation of these kinds of design systems is that, the user is also required to be always online in order to check the mail containing attachment of the captured pictures. Hence to overcome this limitation, in this paper, we come up with an idea of introducing an Arduino (microcontroller) in communication with the Raspberry Pi and a GSM Module is interfaced to an Arduino.

This additional design helps in alerting the user with the registered mobile number via SMS or by making a call according to the user requirement indicating to check the E-mail. Hence this avoids the user to be online always. This paper also provides an idea of using Advanced IP Scanner and VNC Viewer software's for identifying the IP address of Raspberry Pi and configuring it effectively in an easier way without complexity.

The architecture of proposed IoT based security alert system is as shown in the Fig. 2. Here the Raspberry Pi, PI Camera and Arduino with the GSM module with power supply forms the entire security system to be deployed at the required place. PIR motion sensor is connected Raspberry Pi through the GPIO pins and the LCD monitor is used for setting up Raspberry web server. The Raspberry Pi and Arduino are made to communicate by connecting them with an USB cable.

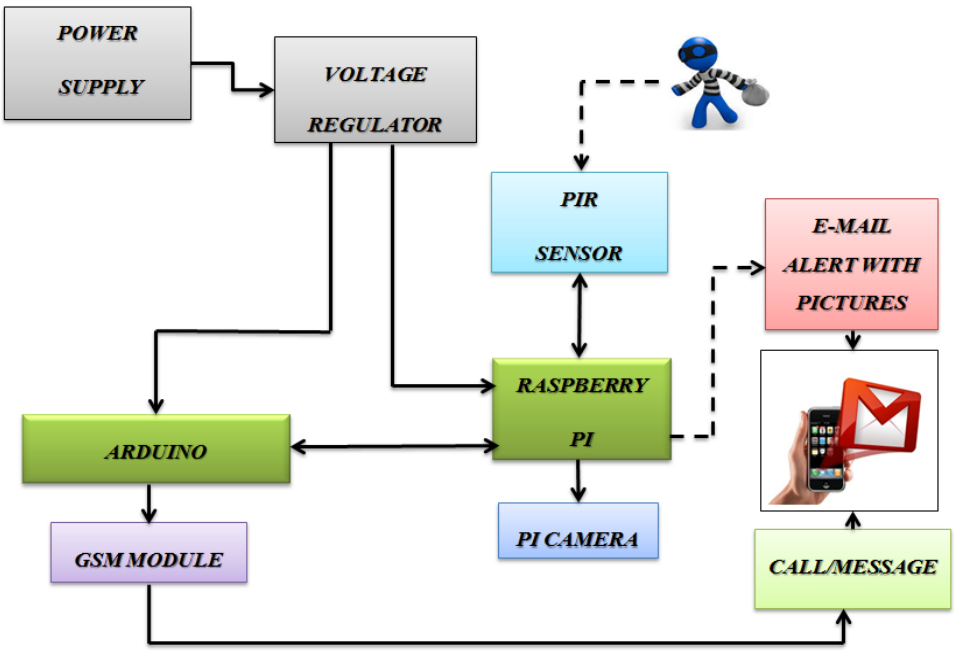

Figure 2: Block Diagram of an IoT Based Intelligent Security System.

The required hardware of the proposed system includes a sensor (PIR Sensor) as an basic input to the system, Raspberry Pi 3B and At-mega2560 (Arduino) microcontrollers for controlling the entire security alert system, PI camera/Web-cam can be used to capture the images when required, and a SIM 900a (GSM module) for sending a SMS or making a call to the specified mobile number. The sensing and detection of an intruder is done with the help of Passive Infrared (PIR) sensor. The infrared rays produced by the human body can be detected by a PIR sensor. Hence if any human motion is sensed and detected, the signals are sent to the microcontroller and are installed in the entrance of the system. Raspberry Pi 3B along with AT-Mega 2560 (Arduino) microcontroller is used as a central controller. It is an 8 bit microcontroller and has 16 MHz crystal oscillator which consists of 54 digital pins and 16 analog pins. On the other hand Raspberry pi 3B has a broadcom BCM2387 chipset with frequency of 1.2GHz Quad-Core ARM Cortex-A53 802.11 b/g/n Wireless LAN and Bluetooth 4.1. Additionally, it adds a wireless LAN and Bluetooth connectivity making it an ideal

solution for powerful connected designs. The use of Raspberry Pi 3B model over other models is that it has an inbuilt camera slot. Hence, PI camera is connected to the provided inbuilt camera slot. It has a micro SD card slot so that the captured images can be stored in it. It also contains Ethernet, GPIO, camera, and display connectors, memory card slot and also video and audio output ports which enables audio and display interfacing. The key benefits of using Raspberry Pi 3B is low cost, consistent board format, added connectivity and 10 times faster processing speed. Finally, GSM module (SIM 900a) is based on Quad-band technology. Quad band of this module are 850/900/1800/1900MHz. It also supports GPRS technology for satellite navigation. Class 10/Class 8 is GPRS multi-slots. AT commands are used to communicate between a mobile phone and a GSM module. Calling a pre-configured number, sending and receiving messages about intrusion detection is done with the help of AT commands.

The required software for the proposed system includes a SD Card Formatter to format the SD card without any cache data, an Advanced IP Scanner to identify the IP address of the connected Raspberry Pi board, a VNC Viewer to configure, program and run the code and a Gmail application on the user's mobile phone.Initially format the SD card by using SD Card Formatter software and then install Raspbian on the micro SD card that will be used in Raspberry Pi and the latest image of Raspbian OS from Raspberry Pi website. After the successful installation of Raspbian OS on Raspberry Pi, the software must be updated by running the certain required Linux commands. Once the software is installed on SD card, the SD card is inserted into the slot in Raspberry Pi. Now to provide the internet connection to the Raspberry Pi, the Advanced IP scanner software must be installed, through which the IP address of the Raspberry Pi board is found and configured through the VNC Viewer software by entering the recognized IP address. Later configure the PI camera and install the software for Email. The Python code for working of the system synchronously to be programmed accordingly on the Python platform. Also, the user's mobile must have an access to the Gmail by installing the application to view the mail with an attachment of the captured pictures.

IV. IMPLEMENTATION AND METHODOLOGY

The most important part of any security system is to accurately detect the visitor who enters and leaves through the entrance. An entrance guard can be managed remotely, detecting visitors at door and alerting to the user on a mobile phone is the most natural way to perform security [6].

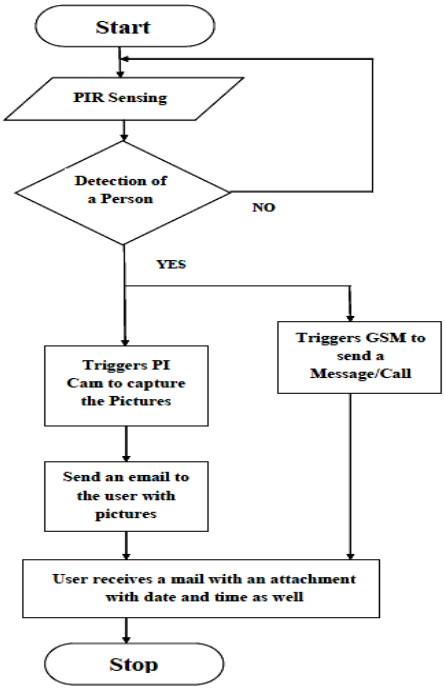

Figure 3: Flow Diagram and Operational Flow of an IoT Based Intelligent Security System.

The remote monitoring and controlling of Embedded Control Unit (ECU) over the internet can be mechanized by setting up certain network architectural design communication standards. Fig. 3 shows the operational flow of the designed security alert system which uses the required commands and program for the effective and synchronous functioning of the system [7].

In this security system, a PIR sensor is used to detect the presence of an intruder and a Pi Camera is used to capture images when the presence it detected. Whenever an intruder comes in range of PIR sensor, PIR Sensor triggers Pi Camera through Raspberry Pi**.** Raspberry pi sends commands to Pi camera to click picture and saves the picture in the memory card inserted into Raspberry Pi. Then, Raspberry Pi triggers GSM module through Arduino and also creates a mail and sends it to the defined mail address with recently clicked images. The images captured will be directly streamed on user's pre-decided Gmail on smart phone. The mail contains a message as "Please find the attachment" along with pictures of intruder as an attachment. Here the pictures are saved in Raspberry Pi with the name which itself contains the time and date of entry. So that we can check the time and date of intruder entry by just looking at the picture name. Since user will not be available online, simultaneously the GSM module is used to alarm the registered mobile user either by SMS or making a call based on user requirement to check the Email [8][9].

V. EXPERIMENTAL RESULTS

The proposed design system is tested in the real environment by deploying it in the required place.

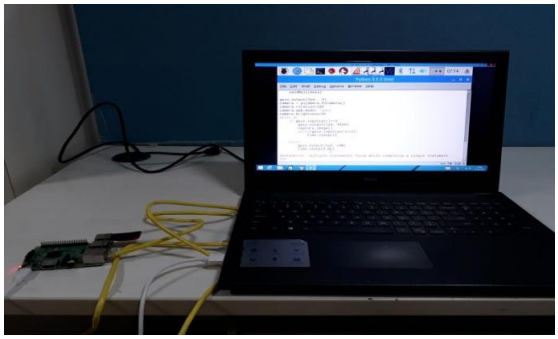

Figure 4:The Experimental Setup of the System.

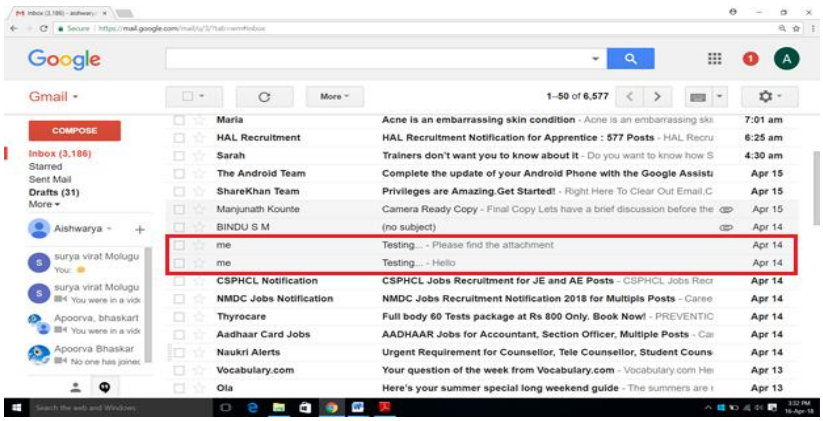

Figure 5: The Mail Obtained when the Intruder is Sensed and Detected.

We have considered two different scenarios to validate proposed approach. In scenario 1, system monitors the room with motion sensors, camera and an intruder is detected by system as shown in Fig. 4. In scenario 2, system sends captured images to owner via email as shown in Fig. 5.

VI. CONCLUSION AND FUTURE WORK

This paper presents the design and implementation of an IoT based intelligent security system with an Email alert. It can be concluded that the proposed system present the basic level of home security and remote monitoring while the required objectives of home security system have been achieved. This security system has minimum delay during process of email alert. This paper also confirms the advantage of Raspberry Pi as the flexibility in terms of cost and broad probability of its usage. Preliminary analysis has shown encouraging results. The proposed design system has an advantage of alerting and noticing the user remotely about the theft caused even when the user is not online by a SMS or call via GSM module. The limitation is that, a SMS or a call can be successful only when there is a good network without any problem of network services. The designed system finds its applications in Smart Homes or also can be installed at the entrance of home or office doors. The future scope of the proposed system can be a RFID tag reader or a Fingerprint sensor to be deployed at the entrance, in order to provide an easy access to the owner to enter the house or an office.

REFERENCES

[1] X. Xu, "*Study on security problems and key technologies of the internet of things*," Proc. - 2013 Int. Conf. Comput. Inf. Sci. ICCIS 2013, pp. 407–410, 2013.

[2] M. M. Hossain, M. Fotouhi, and R. Hasan, "*Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things*," 2015 IEEE World Congr. Serv., pp. 21–28, 2015.

[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "*A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications*," IEEE Internet Things J., *vol. 4, no. 5*, pp. 1125–1142, 2017.

[4] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "*IoT based smart security and home automation system*," 2016 Int. Conf. Comput. Commun. Autom., pp. 1286–1289, 2016.

[5] S. Anwar and D. Kishore, "*IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone*," *vol. 5, no. 12*, pp. 504–509, 2016.

[6] M. Shariqsuhail, G. Viswanathareddy, G. Rambabu, C. V. R. Dharmasavarni, and V. K. Mittal, "*Multi-functional secured smart home*," 2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016, pp. 2629–2634, 2016.

[7] S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, and M. S. Obaidat, "*An advanced Internet of Thing based Security Alert System for Smart Home*," IEEE CITS 2017 - 2017 Int. Conf. Comput. Inf. Telecommun. Syst., pp. 25–29, 2017.

[8] D. Shital and N. Prof, "*Management for Smart Home System*," IEEE ICECA 2017 pp. 552–556, 2017.

[9] Molugu Surya Virat, Aishwarya B, Bindu S M, Dhanush B N and Manjunath R Kounte. "*Security and Privacy Challenges in Internet of Things*", International Conference on Trends in Electronics and Informatics, 11-12, May 2018 [Accepted].