International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 2, Mar- Apr 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Implementation of Internet of Things (IoT) Based Access Control System

Engr. Nwunkor Frances
Electrical and Electronic Engineering Department
Petroleum Training Institute (PTI), Effurun
Delta State, Nigeria.
francesnwukor@gmail.com

----------**********----------

Abstract:

The deployment of IoT on smart devices is based on the ease of user in accessing and controlling the system remotely via internet. By using IoT system in case of access control, users can access and control entrance point in 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 remote monitoring based on IoT is very important for wide range of commercial and security application. It is necessary to develop a framework that control and monitor users access to a facility remotely. Hence, this paper presents an implementation of IoT based access control system, in which the system detects the presence of a human and sends a notification containing the pictures of the human with date and time to a mobile app, the user can decide to grant access or not via the mobile app.

Keywords:- **IOT, Security, Access, Control, Entrance, Remote, Notification, Arduino**

----------**********----------

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 [2]. 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 [3]. 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 [4]

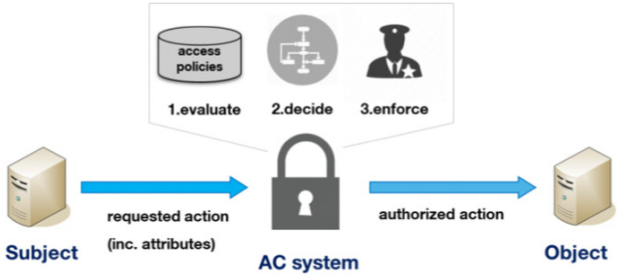

Fig.2: IoT Architecture

II. SYSTEM ARCHITECTURE

The system, IoT based Access control system consists of two parts, Embedded Control system Unit (ECU) and Remote Control Unit (RCU) is a user interfaced implemented on Users smart phone.

A. Embedded Control Unit (ECU) ECU is an efficient, low power consumption and low cost The ECU allows user to remote monitoring and controlling. ECU consists of Arduino board set up with code. GSM/GPRS, PIR motion sensor and image sensor interfaced with Arduino Uno to detect visitor's motion at Door and capture image respectively. Captured images with time and date are saved on Server. Arduino is configured for enabled SSH and camera. ECU also consists of Relay Driver for control of Electromagnetic Door lock and Loud Speaker system for enabled Voice alert.

B. Remote Control Unit (RCU) RCU is a software tool implemented on Users Smart Phone. Provide GUI (Graphical User Interface) to send predefined Terminal Commands via SSH to ECU. SSH is a secure protocol and the most commonly used to administrate and communicate with servers. RCU is implemented on android platform using Java Script on JDK (Java Development Kit) and Andriod Studio IDE.

III. BLOCK DIAGRAM

The System block diagram of IoT based Access control System is shown in figure 1. It comprises of various units which are Image Sensor, PIR, GSM module and arduino board.

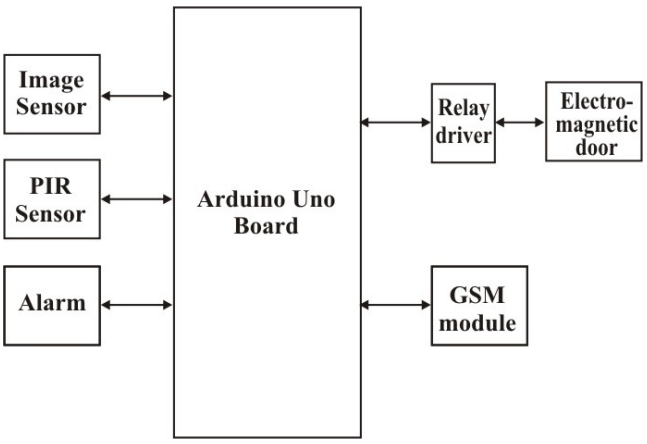

Fig.2: Block diagram of IoT Based Access Control

C. *Methodology*

The methodology employed in realizing electric kettle with automatic temperature indicator includes the subsequent steps:

i. Study of previous literatures on the project to better understand the concept and functionality of the project.
ii. Understanding the entire system of hardware and software sequences.
iii. Designing the system circuit and developing the control algorithm.
iv. Testing the functionality of the varied sections of the system.
v. Combining the both hardware and software components of the system.
vi. Documenting the Research/Project

IV. SYSTEM COMPONET DESCRIPTION

A. Image Sensor (OV7670)

The OV7670 image sensor is a small size, low voltage, single-chip VGA camera and CMOS image processor for all functions. It provides full-frame, sub-sampled or windowed 8-bit images in various formats, controlled through the Serial Camera Control Bus (SCCB) interface.

The camera module is powered from a single +3.3V power supply, and external clock source for camera module XCLK pin. The OV7670 camera module built-in onboard LDO regulator only requires single 3.3V power and can be used in Arduino, STM32, Chipkit, ARM, DSP, FPGA an d etc.

Fig.3: The OV7670 image sensor

OV7670 module specification:

- Optical size 1/6 inch
- Resolution 640×480 VGA
- Onboard regulator, only single 3.3V supply needed
- Mounted with high quality F1.8 / 6mm lens
- High sensitivity for low-light operation
- VarioPixel® method for sub-sampling
- Automatic image control functions including: Automatic
- Exposure Control (AEC), Automatic Gain Control (AGC), Automatic White Balance (AWB), Automatic
- Band Filter (ABF), and Automatic Black-Level Calibration (ABLC)
- Image quality controls including color saturation, hue, gamma, sharpness (edge enhancement), and anti-blooming
- ISP includes noise reduction and defect correction
- Supports LED and flash strobe mode
- Supports scaling
- Lens shading correction
- Flicker (50/60 Hz) auto detection
- Saturation level auto adjust (UV adjust)
- Edge enhancement level auto adjust
- De-noise level auto adjust

The connection between the module and the Arduino uses 6 analog pins and 8 digital pins, and they have to be connected as shown in this figure 4

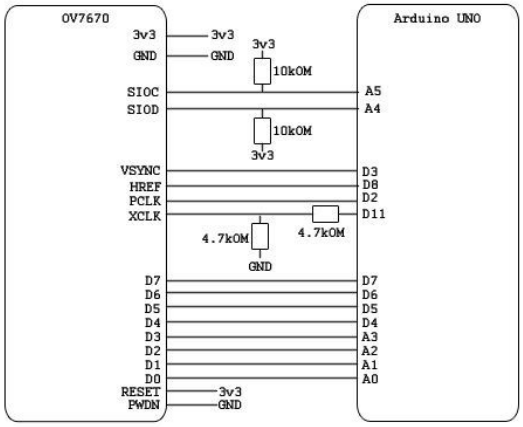

Fig.4: Arduino interfaced with OV7670 image sensor

B. PIR Motion Sensor

This access control system is also based on PIR motion sensor and arduino interfacing. By using the PIR sensor, the system can detect the trespassers and intruders entering in the restricted area.

When a motion is detected by the PIR sensor it sends the signal to the arduino. Once receiving the signal arduino triggers the alarm ON. The main aim of this project is to deter the trespassers and intruder.

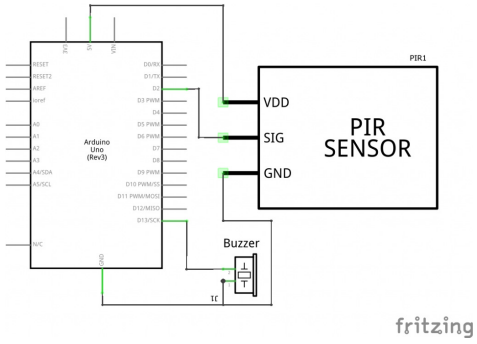

Fig.5: Arduino interfaced with PIR sensor

C. SIM900A GSM/GPRS Module

SIM900A Modem can work with any GSM network operator SIM card just like a mobile phone with its own unique phone number.

SIM900A GSM/GPRS modem is plug and play modem with RS232 serial communication supported. Hence Advantage of using this modem will be that its RS232 port can be used to communicate and develop embedded applications.

Applications like SMS Control, data transfer, remote control and logging can be developed. SIM900 modem supports features like voice call, SMS, Data/Fax, GPRS etc.

SIM900A modem uses AT commands to work with supported features.

To be connected to a cellular network, the modem requires a SIM card provided by a network provider.

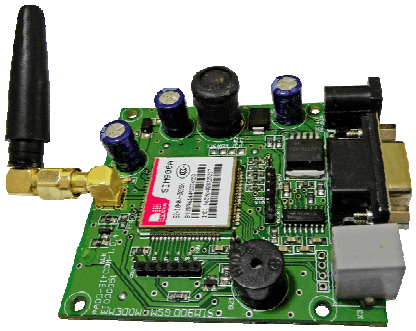

Fig.6: SIM900A GSM/GPRS Module

TCP Client using SIM900A GPRS and Arduino UNO

- SIM900 enables GPRS connectivity to embedded applications. We can

implement TCP Client protocol using SIM900 TCP function AT Commands.

- The Transmission Control Protocol (TCP) is standard transport layer internet protocol which used in establishing and maintaining communication in between server and client.
- It is widely used in IoT (Internet of Things) embedded applications, where every sensor is connected to a server and we have access to control them over the internet.
- The GSM/GPRS module uses USART communication to communicate with microcontroller or PC terminal. AT commands are used to configure the module in different modes and to perform various functions like calling, posting data to a site, etc.

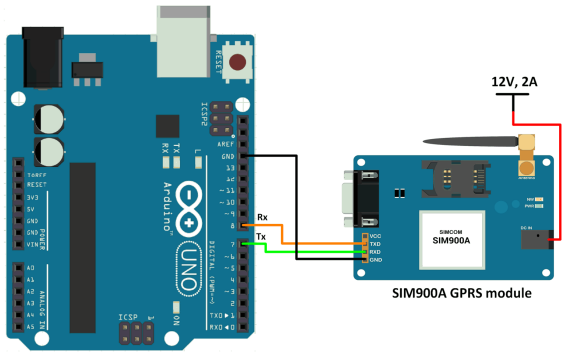

Fig.7:Arduino Interfaced with GSM/GPRS Module

III. THE SYSTEM SOFTWARE DESIGN

a. Flow Chart

The flow chart gives a graphical representation of the sequence of program execution. The executional flow chart is given below:

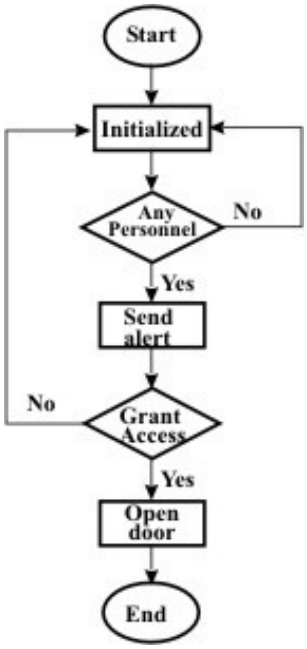

Fig.8 Flow chart of the program.

V. RESULT

The experimental setup to monitor the access way for visitor was tested unit by unit for functionality.

Alert: the PIR sensing the presence of an object (visitor) send a signal which represents a high (1) to the microcontroller and whenever the microcontroller receive high from the PIR it will send a signal to the camera to shot. A notification message containing the image of the object and time will be immediately sent to the android App where the user is been prompted to grant or deny access. The user can also activate the loud speaker to deter in case of an intruder. The user then sent command using android GUI over Internet to ECU for controlling actions based on command sent to ECU to activate respective devices. For example, a command with the subject ON CAMERA ALERT was sent to ECU to active Image Sensor, capture image and there is usually a notification if anybody is found at access way or door.

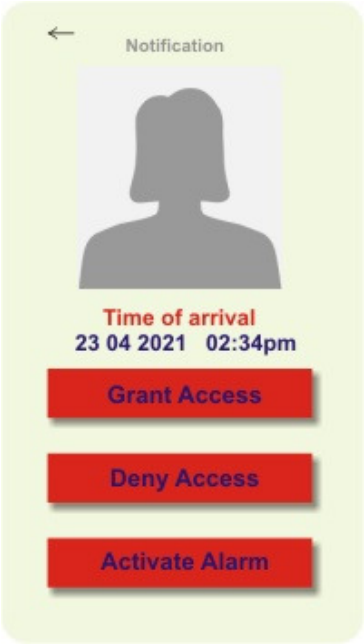

Fig.9: Notification Page

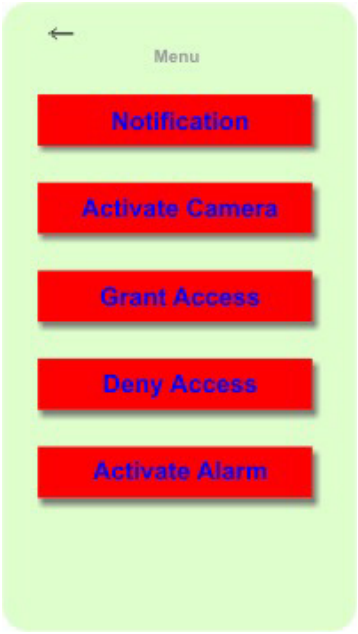

Fig.10: Main Menu

Fig.11: Access granted page

Fig.12: Alarm

VI. CONCLUSIONS

This paper presents the design and implementation of an IoT based access control system with notification. It can be concluded that the proposed system present the basic level of security and remote monitoring while the required objectives of the access control system have been achieved. This control and monitoring system has minimum delay during process of notification. Preliminary analysis has shown encouraging results. The proposed design system has an advantage of alerting and noticing the user remotely about an intruder caused provided there is an internet network. The designed system finds its applications in homes or also can be installed at the entrance of home or office doors, banks, police stations. 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.

ACKNOWLEDGMENT

My gratitude to God almighty for the strength to complete this journal and also to my family for their love.

REFERENCES

[1] Aishwarya B, Bindu S M, Molugu Surya Virat, Manjunath R Kounte "*Design And Implementation Of Iot Based Intelligent Security System*" IJARSE, volume no.: 07, April 2018, pp. 290 – 297, 2018.

[2] 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.

[3] [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.

[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] Xiaohui, Xu. (2013). Study on Security Problems and Key Technologies of the Internet of Things. 407-410. 10.1109/ICCIS.2013.114.

