Wireless Home Security and Monitoring System

*

Md. Masbahul Hasan
dept. Information and Communication Technology
Bangabandhu Sheikh Mujibur Rahman Digital University
Kaliakor, Gazipur, Dhaka, Bangladesh
1901014@iot.bdu.ac.bd

Marshia Muntaka
dept. Information and Communication Technology
Bangabandhu Sheikh Mujibur Rahman Digital University
Kaliakor, Gazipur, Dhaka, Bangladesh
1901021@iot.bdu.ac.bd

Tasnima Hamid
dept. Information and Communication Technology
Bangabandhu Sheikh Mujibur Rahman Digital University
Kaliakor, Gazipur, Dhaka, Bangladesh
1901043@iot.bdu.ac.bd

***Abstract*—The main aim of this paper is to make our homes smarter and more secured. the technology or concept for this paper is basically IOT and cloud-based services which are a thing of present and future. Home automation. system has achieved much more popularity in the past decades has focused on mainly improving quality of life overall. The IOT based devices will help in surveillance and energy management and also provides support for a direct message or SMS to nearby friends and support with GPS location and predefined message just by a single tap of user. All these operations are controlled by cloud system with active internet support.**

***Index Terms*—security, home automation, authentication, key, sensors, IOT, devices, Cloud, Data.**

INTRODUCTION

Everyone wants their assets to be protected from threats and harm. People want security in everyplace possible when they are away from their homes. In 21st century crime rates have got increased and people want security so This system is designed in that way to provide automated advance security for their homes. Home automation system has grown rapidly, which provide us with convenience, comfort and mainly quality of life and focus on security for all the residents. people are habitual of automated devices, which are commonly known as smart devices, with the rapid development in the field of technology everyday new devices are created, the IOT has also emerge as boost up to make smart device even smarter. In today's era most homes consist of electrical devices which are controlled manually but with evolution of IOT these devices made the working simpler and controllable by automation. Today the main concern is security. With the use of these IOT based devices security can be achieved and full equipped home security measures can betaken. This paper focus on working and implementation of some techniques and methods of home automation for security which are already existed and compares the time cost and speed and functionalities. Markets are full of many home automation technologies; our research paper compares some existing technology and has selected a choice of available technology and highlight their drawbacks and advantages. The rest of the paper has following sections which will cover the applications of Tech used and its advantage and drawbacks in our paper and also covers all the methodial of our research and further we will conclude in our last section. All the applications are now cloud based support and devices itself are cloud oriented and connected to all the nearby devices. internet of things is just interconnection of all the connected devices with each other to share data and to make things easier These types of devices are now well equipped with performing actions which are not possible earlier. The main point here is now devices are more capable of doing thing in protecting our home and surveillance.

I. LITERATURE REVIEW

Security is the main concern for all of us and we live in an era where everything is connected to internet and to keep our self-secure, we use security systems which are a part of IOT and Cloud technology. Iot is connecting our small to small devices to Internet, this type of innovation has helped in creating security solutions for our homes the concept of IOT is to create a virtual connection between a centralized device and network devices. This virtual connection helps in locating and tracking and controlling connected objects. device-to - device connectivity, the concept of development of smart sensors together with many communication technologies such as Bluetooth, Wi-Fi etc. are all supported by way of cloud computing technologies.A well-designed security system implemented should have the following important ideas. Firstly, the system should be made in this way that it is aware of the perpetrator. The home owner should get instant alerted text so in order to take some actions. Finally, there should be an active device to record all these events, which could help everyone later be used to carry out search for thieves and stolen things the type of alert mechanism will be used as a cellular device like a portable.[1] To alert the owner cloud message or SMS services

will be used. The mechanism to alert owners and others people is used as a measure. The concept of Short message system [SMS] is used to alert. the owner.[2] Generally, this setup has three components: A Global System for Mobile module, A Microcontroller and different type of Sensors in an arranged manner. [3] [4]. Biometric authentication Security Systems can be implemented through capturing of retina and fingerprint data that can be passed through a secure server. [5] [6]. The system design comprises of many ways to get notify the user for any malicious activities occurred within its sensor range, A high pitched sound buzzer alarm that activates and everyone nearby understands that security is being compromised.[11]. The design consists of a smart phone which is of android operating system with support of android application for home automation, and Arduino Additional Decryption Key Computing [ADK] The sensors and embedded devices are managed by user which sends signals with their smartphones managing and controlling all activities from far places [7]. It consists of a set of arrangement of devices during a case where the operations of operating and managing them can be done by user just by a single tap, and when a situation came where a server is down or no connection is available and user cant access all the appliance's and system's then also a system work itself with an attached Arduino board which consist of predefined codes and can operate itself still securing our assets[8]. Home security and automation systems have increased rapidly and in future its demand will be high they are available for every level of income and suitable lifestyle.[12] Home security is very much important for our own protection and convenience. The aims of paper are to develop a system which is fairly affordable reliable which ensure proper protection and applies to our home security system exploitation of detectors like pressure and motion detectors. Arduino board is regularly collecting and processing all the data from the sensors and keeps on processing and it act as a microcontroller. In case of some unauthorizes access all the alarm and alert systems will get activated and a message is sent to all the people which are predefined by the owner, so this system is ensuring and securing our home [9].

II. PROPOSED METHOD

A. *WORKING*

The working methodology of the system is as follows

- The system uses RFID system to automate and secure the door lock.
- The system reads humidity and temperature value and displays it using Blynk.
- The system detects gas percentage and gives alert notification if it exceeds safe range.
- The system checks for presence of fire and gives alert.
- The BLynk web and mobile dashboard were configured.

B. *MATERIALS*

1.1. Required Software:

- Arduino IDE
- Blynk

1.1. Required Hardware:

- ESP8266
- Gas sensor(MQ2)
- Flame sensor
- RFID
- DHT11
- Jumper wires
- Relay
- 9v Battery
- Solenoid door lock
- Breadboard

III. SENSOR DETAILS

Fig. 1. ESP8266

- ESP8266
  Espressif Systems in Shanghai, China, manufactures the ESP8266, a low-cost Wi-Fi microprocessor with integrated TCP/IP networking software and microcontroller capabilities. The ESP-01 module, created by an independent manufacturer named Ai-Thinker, helped the chip gain popularity in the English-speaking maker community in August 2014. With the use of Hayes-style commands, this tiny module enables microcontrollers to join a Wi-Fi network and establish straightforward TCP/IP connections. Nevertheless, at initially, there was hardly any information available in English on the chip and the orders it would receive.
- RFID module

Fig. 2. RFID MODULE

Fig. 3. GAS SENSOR

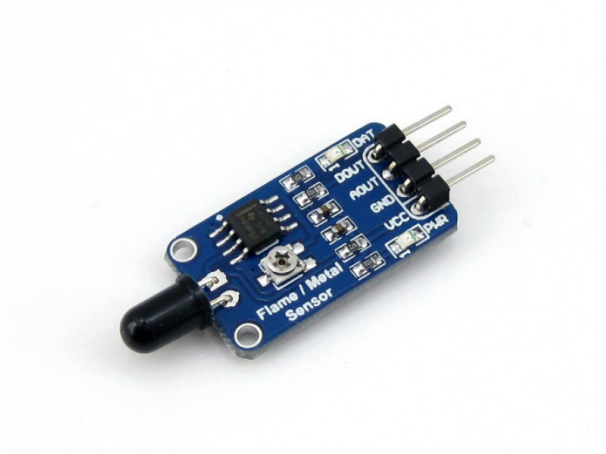


Fig. 4. FLAME SENSOR

RFID (radio frequency identification) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers – fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

- Gas Sensor(MQ2)
  A device that detects the presence or concentration of gases in the atmosphere is called a gas sensor. By altering the resistance of the material inside the sensor, the sensor generates a corresponding potential difference based on the gas concentration, which may be recorded as output voltage. The type and concentration of the gas can be inferred from this voltage value. MQ2 sensor senses LPG gases.
- Flame Sensor
  A flame-sensor is one kind of detector which is mainly designed for detecting as well as responding to the occurrence of a fire or flame. The flame detection response can depend on its fitting. It includes an alarm system, a natural gas line, propane a fire suppression system. This sensor is used in industrial boilers. The main function of this is to give authentication whether the boiler is properly working or not. The response of these sensors is faster as well as more accurate compare with a heat/smoke detector because of its mechanism while detecting the flame.
- DHT11
  The DHT11 sensor comprises of a thermistor for measuring temperature and a capacitive humidity sensing device. The humidity detecting capacitor consists of two electrodes separated by a substrate that can hold moisture as a dielectric. The capacitance value changes as the humidity levels fluctuate. The IC calculates, interprets,

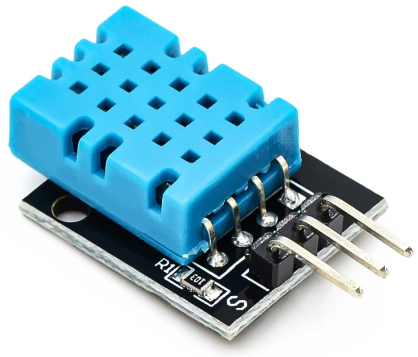


Fig. 5. DHT11

and converts the modified resistance values into digital form. For measuring temperature this sensor uses a Negative Temperature coefficient thermistor, which causes a decrease in its resistance value with increase in temperature. To get larger resistance value even for the smallest change in temperature, this sensor is usually made up of semiconductor ceramics or polymers. The temperature range of DHT11 is from 0 to 50 degree Celsius with a 2-degree accuracy. Humidity range of this sensor is from 20 to 80

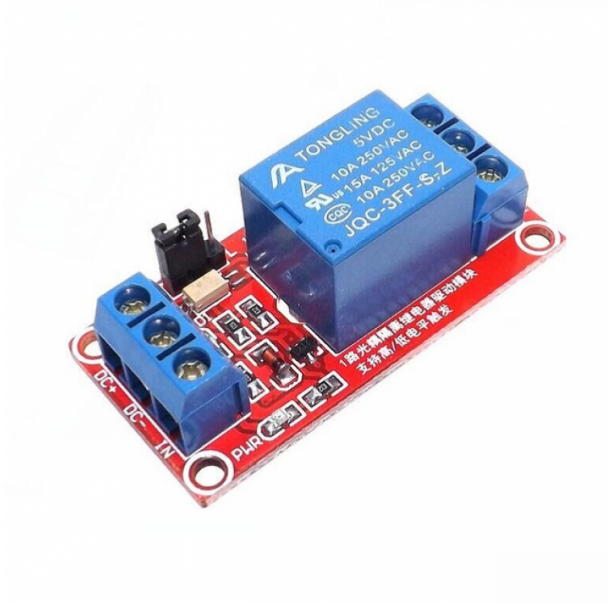


Fig. 6. RELAY

- Relay

Single or Two Channel 5V Relay Module is a relay interface board that can be controlled directly by a wide range of microcontrollers such as Arduino, AVR, PIC, ARM, and so on. It uses a low-level triggered control signal (3.3 – 5V DC) to control the relay.
The electro-mechanical component known as a relay serves as a switch in some situations. In order to open or close contact switches, DC is used to energize the relay coil. A coil and two contacts, such as ordinarily open (NO) and usually closed (NC), are often found in a single-channel 5V relay module (NC). A 5v relay is an automatic switch that is commonly used in an automatic control circuit to control a high-current using a low-current signal. The input voltage of the 5V Relay Module signal ranges from 0 to 5V.

Fig. 7. SOLENOID

- Solenoid Lock
  9V Solenoid lock are basically electromagnets: they are made of a big coil of copper wire with an armature (a slug of metal) in the middle. When the coil is energized, the slug is pulled into the center of the coil. This makes the solenoid able to pull from one end. This solenoid lock in particular is nice and strong, and has a slug with a slanted cut and a good mounting bracket. It's basically an electronic lock, designed for a basic cabinet or safe or door. Normally the lock is active so you can't open the door because the solenoid slug is in the way. It does not use any power in this state. When 9-12VDC is applied, the slug pulls in so it doesn't stick out anymore and the door can be opened. The solenoid lock come with the slanted slug as shown above, but you can open it with the two Phillips-head screws and turn it around so its rotated 90, 180 or 270 degrees so that it matches the door you want to use it with

Fig. 8. Jumper Wire

- Jumper Wire
  We have used Jumper wires as the connecting wires in this project. Jumper wires are simply wires that have connector pins at each end, allowing them to be used to connect two points to each other without soldering. Jumper wires are typically used with breadboards and other prototyping tools in order to make it easy to change a circuit as needed. Fairly simple. In fact, it doesn't get much more basic than jumper wires.Though jumper wires come in a variety of colors, the colors don't actually mean anything. This means that a red jumper wire is technically the same as a black one. But the colors can be used to your advantage in order to differentiate between types of connections, such as ground or power. The jumper is an electrical wire, or group of them in a cable, with a pin at each end, which is normally used to interconnect the components of a breadboard internally or with other components or equipment's without soldering. Individual jump wires are fitted by inserting their "end connectors" into the slots provided in a breadboard, the header connector of a circuit board or a piece of test component.

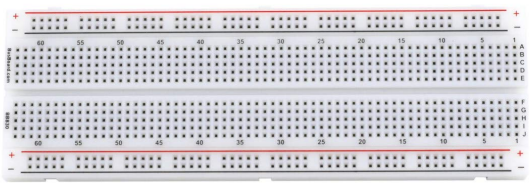


Fig. 9. Breadboard

- Breadboard
  Breadboard, or proto board, is a construction base for prototyping of electronics. Originally the word referred to a literal bread board, a polished piece of wood used when slicing bread.In the1970s the solder less bread-board(a.k.a.plug board, a terminal array board) became available and nowadays the term "breadboard" is commonly used to refer to these. Because the solder less breadboard does not require soldering,it is reusable.This makes it easy to use for creating temporary prototypes and experimenting with circuit design. For this reason, solder less breadboards are also popular with students and in technological education. Older breadboard types did not have this property. A strip board (Veroboard) and similar prototyping printed circuit boards which are used to build semi-permanent soldered prototypes or one-offs, cannot easily be reused. A variety of electronic systems may be proto typed by using breadboards, from small analog and digital circuits to complete central processing units (CPUs). Compared to more permanent circuit connection methods, modern breadboards have high parasitic capacitance, relatively high resistance,and less reliable connections,which are subject to jostle and physical degradation. Signaling is limited to about 10 MHz, and not everything works properly even well below that frequency. A common use in the system on a chip (SoC) era is to obtain an microcontroller (MCU) on a pre-assembled printed circuit board (PCB) which exposes an array of input/output (IO) pins in a header suitable to plug into a breadboard, and then to prototype a circuit which exploits one or more of the MCU's peripherals, such as general-purpose input/output (GPIO), UART/USART serial transceivers, analog-to-digital converter (ADC), digitalto-analog converter (DAC), pulse width modulation (PWM; used in motor control), Serial Peripheral Interface (SPI), or I2C. Firmware is then developed for the MCU to test, debug, and interact with the circuit prototype. High frequency operation is then largely confined to the SoC's PCB.

IV. Results and Discussion

The RFID module automated the door lock system and secured access of members. It uses the Relay and triggers the lock to open it if permitted card is scanned by RFID. Otherwise, it doesn't trigger the lock.

This is the web dashboard the user views. Here, temperature, humidity, gas percentage, and fire state are shown. The user can view it anywhere in the world with the internet.

This is the mobile dashboard the user views. Here, temperature, humidity, gas percentage, and fire state are shown. The user can view it anywhere in the world with the internet.

The system sends notification(push, alert and email) to the user if the gas or fire state is in danger state. It also gives mail to the owner.

Thus the members of the family can stay safe from burglars or robbers. They can also keep them slert and safe using the

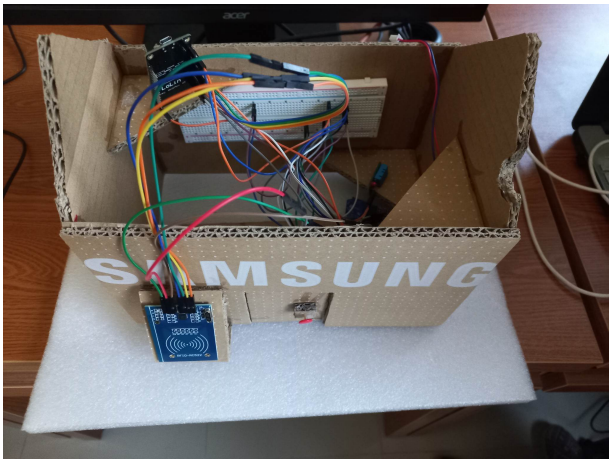
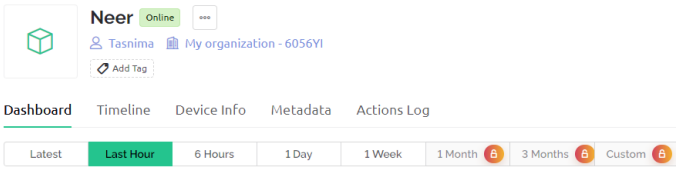


Fig. 10. Prototype



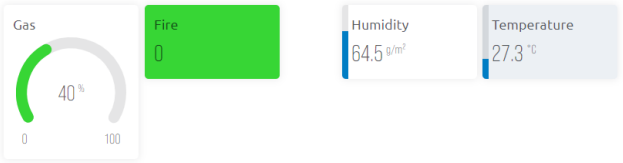


Fig. 11. Web Dashboard

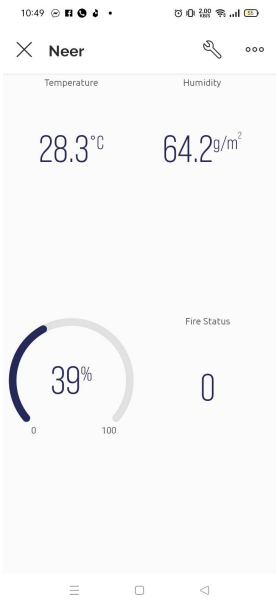


Fig. 12. Mobile Dashboard

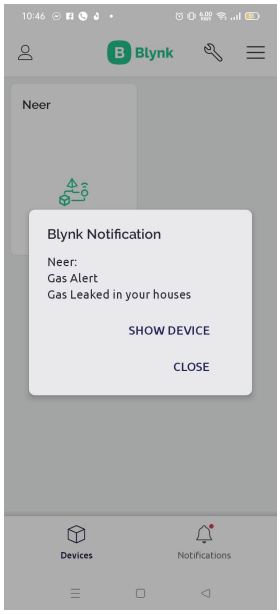


Fig. 13. Alert Notification

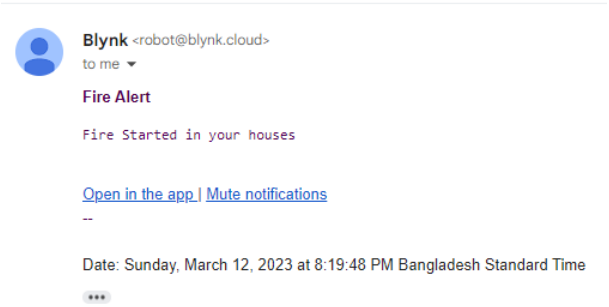


Fig. 14. Alert Notification

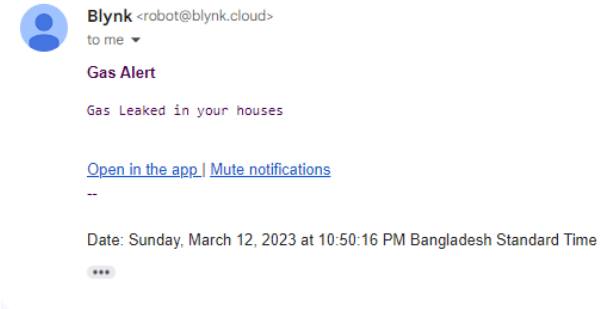


Fig. 15. Alert Notification

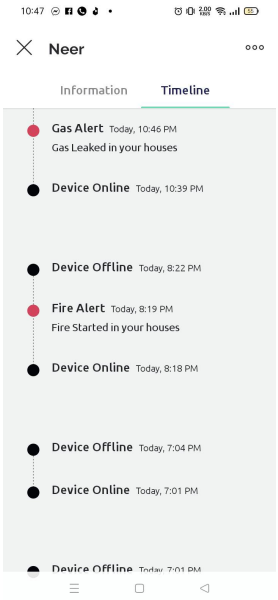


Fig. 16. Device Event Timeline

notifications and monitoring system in Blynk web and mobile dashboard.

V. CONCLUSION

Home automation has taken us to far from traditional ways and increased advancement has led us to use our homes and devices within to optimum level. Future homes will most likely offer practical and advance security to its owners and revolution in smart homes is made possible through IOT devices As we move into the people to come, an ever increasing number of gadgets will start to associate with each other. The fantasy is a future in which information is conveyed among gadgets and people without depending on manual contribution of individual bytes. PCs that can consequently mine information and after that utilization that information to change parts of the home condition is what's to come. For instance, a shrewd indoor regulator that can naturally check the temperature of a room and after that alter the focal warming and cooling units as fundamental or a clothes washer that consequently recognizes its substance and projects itself to be done washing at a predefined time. These are generally objectives that engineers are moving in the direction of and depend on advances in information mining advances as well as in enormous information figuring. Perk of this is the cutting edge home computerization development, that gives you a chance to control, screen and secure your home with your cell phone. The future of home security is at the top and everything is secured and connected to cloud people will feel more safe and get far from homes without worrying about their assets .As advances keep on propelling, you can anticipate that the place of tomorrow should be significantly more computerized than that of today The design consists of Android phone with home automation application, Arduino Mega ADK. User can interact with the android phone and send control signal to the Arduino ADK which in turn will control other embedded devices/sensors. We have discussed a simple prototype in this paper but in future it can be expanded to many other areas.

ACKNOWLEDGMENT

It is our great fortune that we have got opportunity to carry out this project work under the supervision of our honourable Md. Habibur Rahman (Lecturer, Dept. of ICT, BDU)Sir and Farzana Akter (Lecturer, dept. of ICT, BDU) Ma'am. We express our sincere thanks and deepest sense of gratitude to my guide for their constant support, unparalleled guidance and limitless encouragement. We wish to convey my gratitude to our Head of Department madam, Department of ICT, BDU and to the authority of BDU for providing all kinds of infrastructural facility towards the project work.

REFERENCES

[1] Sandip Das '' Home Automation Using Internet of Thing" Department of Electronics and Communication Engineering University of Engineering and Management Jaipur, Rajasthan, India

[2] Mircea Murar and Stelian Brad," Monitoring and controlling of smart equipments using Android compatible devices towards IoT applications and services in manufacturing industry", Automation, Quality and Testing, Robotics, 2014 IEEE International Conference, Cluj-Napoca, pp. 1-5.

[3] Takeshi Yashiro, Shinsuke Kobayashi, Noboru Koshizuka and Ken Sakamura, "An Internet of Things (IoT) Architecture for Embedded Appliances", Electrical and Control Engineering (ICECE), 2011 International Conference, Yichang, IEEE, 2011, pp. 2578-2581.

[4] Keertikumar M. J, Shubham M. and R.M. Banakar, "Evolution of IoT in Smart Vehicles: An Overview", IEEE Computer Society, pp. 804- 809.

[5] Takayuki Suyama, Yasue Kishino and Futoshi Naya "Abstracting IoT devices using virtual machine for wireless sensor nodes", Internet of Things (WF-IoT), 2014 IEEE World Forum, Seoul,2014, pp. 367-368

[6] Seung-Chul Son, Nak-Woo Kim, Byung-Tak Lee, Chae Ho Cho, and Jo Woon Chong "A Time Synchronization Technique for CoAP-based Home Automation Systems", IEEE Transactions on Consumer Electronics,February 2016, Vol. 62, No. 1, pp. 10-16.

[7] Seung-Chul Son, Nak-Woo Kim, Byung-Tak Lee, Chae Ho Cho, and Jo Woon Chong "A Time Synchronization Technique for CoAP-based Home Automation Systems", IEEE Transactions on Consumer Electronics,February 2016, Vol. 62, No. 1, pp. 10-16.

[8] Seungho Chae, Yoonsik Yang, Junghyun Byun and Tack-Don Han "Personal Smart Space : IoT based User recognition and Device control", IEEE Tenth International Conference on Semantic Computing,2016, pp. 182-182.

[9] S.Sujin Issac Samuel "A Review of Connectivity Challenges in IoTSmart Home", 3rd MEC International Conference on Big Data and Smart City,2016.

[10] B. S. S. Tharaniya soundhari, M., "Intelligent interface based speech recognition for home automation using android application," pp. 1 –11, march 2015.

[11] "Wireless Home Monitoring Using Social Internet of Things (SIoT)", Bhagayshree Jadhav, Dr. S.C.Patil, 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)

[12] Learn about Home Automation, available at. http://www.homeauto.comiDownloadslMarketing/Learn$_A bout_H A.pdf$

```
#define BLYNK_TEMPLATE_ID "TMPLItZp_h3z"
#define BLYNK_TEMPLATE_NAME "Neer"
#define BLYNK_AUTH_TOKEN "RDd0XoC0QiDY3j5_hvKj0dN1

#define BLYNK_PRINT Serial
#include <ESP8266WiFi.h>
```

```
#include <BlynkSimpleEsp8266.h>
#include <SPI.h>
#include <MFRC522.h>
//#include <LiquidCrystal_I2C.h>
#include <DHT.h>

//LiquidCrystal_I2C lcd(0x27,20,4);

#define relay_pin 5  ///D1


constexpr uint8_t RST_PIN = D3;
// Configurable, see typical pin layout above
constexpr uint8_t SS_PIN = D4;
// Configurable, see typical pin layout above
MFRC522 rfid(SS_PIN, RST_PIN); // Instance of the class
MFRC522::MIFARE_Key key;
String tag;


char auth[] = BLYNK_AUTH_TOKEN;

char ssid[] = "Tasnima";
// type your wifi name
char pass[] = "12345677";
// type your wifi password

BlynkTimer timer;


#define DHTPIN 15 //Connect Out pin to D2 in NODE MCU
#define DHTTYPE DHT11
DHT dht(DHTPIN, DHTTYPE);

#define gas A0
#define fire 16
#define motionp 2

void sendSensor()
{
  float h = dht.readHumidity();
  float t = dht.readTemperature(); // or dht.readTemperature(true) for Fahrenheit
  float gasvalue = analogRead(gas);
  Serial.println(gasvalue);
  float g = map(gasvalue, 190, 280, 0, 100);
  int f = digitalRead(fire);

  if (isnan(h) || isnan(t)) {
    Serial.println("Failed to read from DHT sensor}");
    return;
  }
  // You can send any value at any time.
  // Please don't send more that 10 values per second.
    Blynk.virtualWrite(V0, h);
    Blynk.virtualWrite(V1, t);
    Blynk.virtualWrite(V2, f);
    Blynk.virtualWrite(V3, g);
    if(f == 1){
      Blynk.logEvent("fire_alert","Fire Started in

    if(g >= 50){
      Blynk.logEvent("gas_alert","Gas Leaked in yo
}
void setup()
{

  Serial.begin(115200);


  Blynk.begin(auth, ssid, pass);
  dht.begin();
  SPI.begin(); // Init SPI bus
  rfid.PCD_Init();
  pinMode(gas, INPUT);
  pinMode(fire, INPUT);
  pinMode(motionp, INPUT);
  pinMode(relay_pin, OUTPUT);
  timer.setInterval(100L, sendSensor);
  //lcd.begin(20, 4);
  //lcd.init();
  //lcd.backlight();
  //lcd.clear();
  //lcd.setCursor(0,0);
  //lcd.print("Welcome to NEER");

}
void loop()
{
  Blynk.run();
  timer.run();
  int motion = digitalRead(motionp);
  if ( ! rfid.PICC_IsNewCardPresent())
    return;
  if (rfid.PICC_ReadCardSerial()) {
    for (byte i = 0; i < 4; i++) {
      tag += rfid.uid.uidByte[i];
    }
    Serial.println(tag);
    if (tag == "1945148151" || tag == "49582230" |
      Serial.println("Access Granted!");
      /**if(tag == "49582230"){
        lcd.setCursor(2,0);
        lcd.print("Hi Mesba!!");
      else if(tag == "2258442"){
        lcd.setCursor(2,0);
        lcd.print("Hi Tasnima!!");
      else if(tag == "9211979"){
        lcd.setCursor(2,0);
        lcd.print("Hi Prottasha!!");
```

```
      }
      else{
        lcd.setCursor(2,0);
        lcd.print("Welcome!");}**/


      digitalWrite(relay_pin, HIGH);
    } else {
      Serial.println("Access Denied!");
      digitalWrite(relay_pin, LOW);
    }
    tag = "";
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
  }
}
```