PAPER • **OPEN ACCESS**

Home security system using internet of things

View the article online for updates and enhancements.

Home security system using internet of things

Anitha A

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: aanitha@vit.ac.in

Abstract IoT refers to the infrastructure of connected physical devices which is growing at a rapid rate as huge number of devices and objects are getting associated to the Internet. Home security is a very useful application of IoT and we are using it to create an inexpensive security system for homes as well as industrial use. The system will inform the owner about any unauthorized entry or whenever the door is opened by sending a notification to the user. After the user gets the notification, he can take the necessary actions. The security system will use a microcontroller known as Arduino Uno to interface between the components, a magnetic Reed sensor to monitor the status, a buzzer for sounding the alarm, and a WiFi module, ESP8266 to connect and communicate using the Internet. The main advantages of such a system includes the ease of setting up, lower costs and low maintenance.

1. 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 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 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.

2. Literature review

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 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.

A novel way to design an electronic lock using Morse code and IoT technology [6]. The authors claim that this as an original idea which have not been tried before and is the first of its kind "optical Morse code-based electronic locking system". This system uses LED's (Light emitting diodes) as an encrypting medium to send signals. To make it more accessible to general public, the LED in smart phones has been used. On the receiver's side is a photosensitive resistor as well as a microcontroller such as arduino processor which has the ability to decrypt the optical signal after receiving them from the LED. Upon decoding the signal it can than upload the current condition of the lock to a cloud from where the owner can monitor the system. The authors have experimented the system in real time and it has proved to work under different illumination environments with all the functions working as they were intended to. The authors also claim to have an easy and user-friendly interface. The IoT system developed here works very well and can be used by anyone and is very convenient due to the use of mobile phones as LED, which also makes it a cost expensive alternative[7]. Anitha et al (2016) proposed an home automation system using artificial intelligence and also proposed a model for cyber security systems [8,9].

3. Materials and Methods

Various hardware materials are required to have an home automation system. Some of the essential components are listed below to have and idea about the proposed system.

3.1. Arduino Uno

Arduino is an open source, PC paraphernalia and programming organization, endeavour, and client group that plans and produce microcontroller packs for constructing programmed devices and intelligent object that can detect and control questions in the real world. The inception of the Arduino extend began at the Interaction Design Institute in Ivrea, Italy. The equipment reference plans are appropriated under a Creative Commons Attribution Share. Arduino Uno is shown in figure 1.
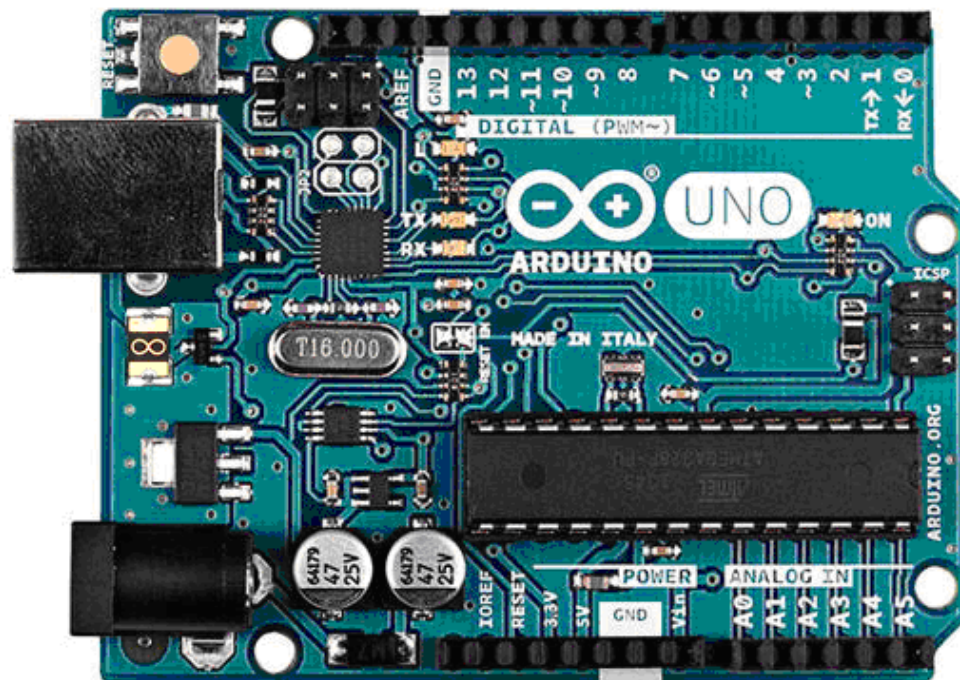
Figure 1. Arduino Uno.
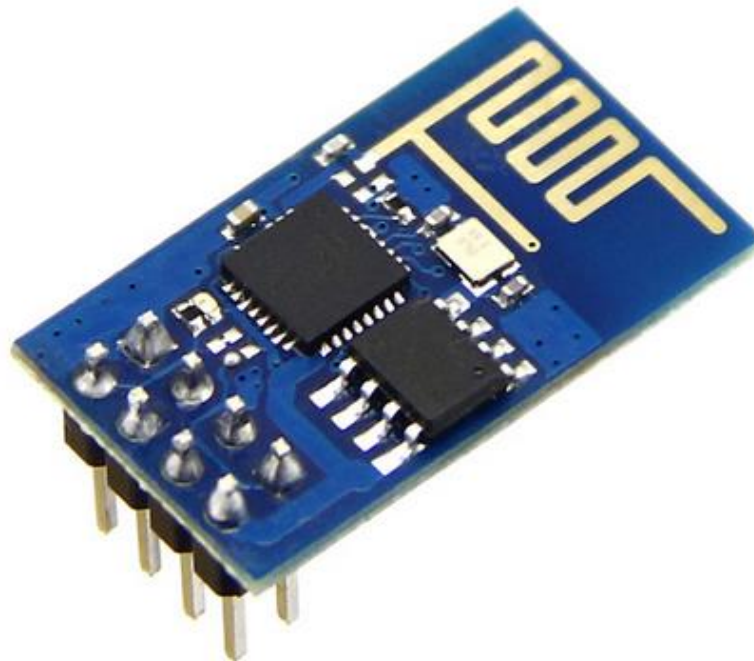
3.2. ESP8266 (WiFi Module)

Figure 2. ESP8266 (WiFi Serial Transceiver).

The ESP8266 is an ease Wi-Fi chip with full TCP/IP stack and MCU (Micro Controller Unit) capacity created by Chinese . These are the primary arrangement of modules made with the ESP8266 by the outsider producer AI-Thinker and remain the most generally available. They are large alluded to as "ESP-xx modules". To shape a workable advancement framework they

require extra parts, particularly a serial TTL-to-USB connector and an outside 3.3 volt control supply. The ESP8266 is shown in figure 2.

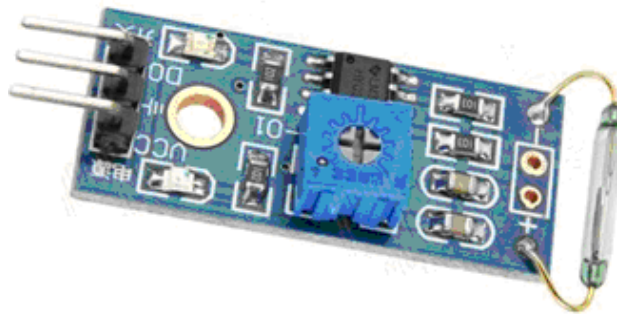### 3.3. Reed Sensor Module

Figure 3. Reed Sensor Module.

In general, an electrical switch known as reed switch, worked by a connected field. It comprises of a fixed glass envelope where there are two ferrous flexible reeds and is loaded with idle gas called rhodium. At the point when an attractive substance ways to deal with the glass envelope, the reeds will meet up because of the attractive field subsequently finishing an electric circuit. At the point when the outer attractive field vanishes, two reeds will be isolated in view of their versatility, the circuit is likewise disconnected. It has been connected in printers, clothes washers, fridges, cameras, door magnets, window magnets, electromagnetic transfers, electronic measuring gadgets, level meters, gas meters, water meters, and so forth. Reed sensor module is shown in figure 3.

3.4. Bread board and Jump wires

A breadboard is utilized to build and test circuits expeditiously afore finalizing any circuit design. The breadboard has many apertures into which route components like ICs and resistors can be connected. The apertures are generally spaced 0.1" apart to put up standard DIP machinery. A typical breadboard that includes top and bottom power distribution rails is shown below figure 4. Jump wires are generally used to establish connectivity with bread board as shown in figure 5.
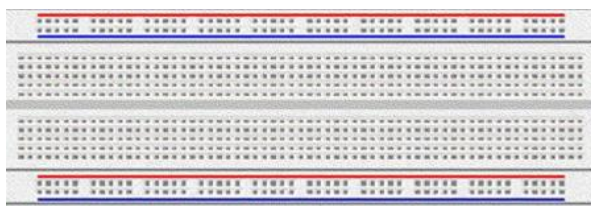

Figure 4. Bread board.   **Figure 5.** Jump Wires.

4. Proposed Working Model

Before we begin connecting the hardware, we have to get the ESP8266 set up by flashing the latest version of the firmware available for the module. This is because the chip comes with an older version of the AT command firmware pre-installed out of the box which cannot communicate with the Blynk libraries efficiently and will give an error with our code. To flash the latest firmware, download the ESP8266 flasher tool and the latest firmware from the

internet which would be in the bin format and set up the ESP8266 to the Arduino Uno as described below in figure 6.

ESP8266	ARDUINO UNO
GND	GND
GP2	Not Connected
GP0	GND
RX	RX
TX	TX
CHPD	3.3 V
RST	Not Connected
VCC	3.3 V

Figure 6. Setup to enable ESP8266 Flash mode.

Once the ESP8266 has been flashed with the latest firmware, other components can be added to the configuration. For this we will need a breadboard to connect the microcontroller, reed sensor, buzzer and the ESP8266 using the jumper wires. The breadboard is used to interface between the various components available. It also makes it easy to connect multiple inputs to a single pin on the arduino board.

Following sketch shown in figure 7, which has been constructed using the Fritzing software shows how the components are supposed to be connected together using the breadboard and the jumper wires. The final configuration need not be identical to the given sketch, although the pins on each device needs to be connected to the same corresponding pins on the Arduino Uno board . The architecture diagram is shown in figure 8.
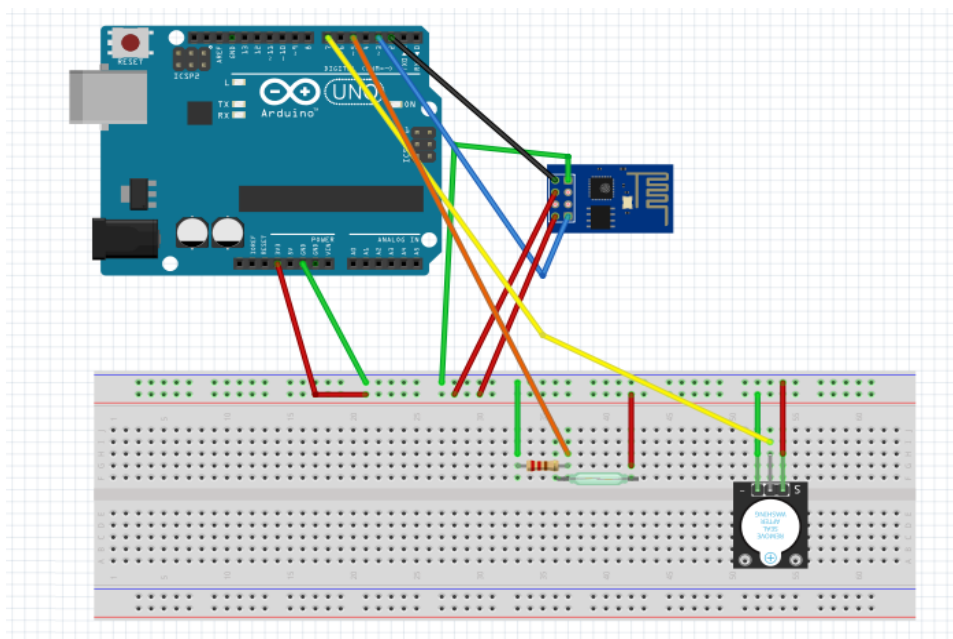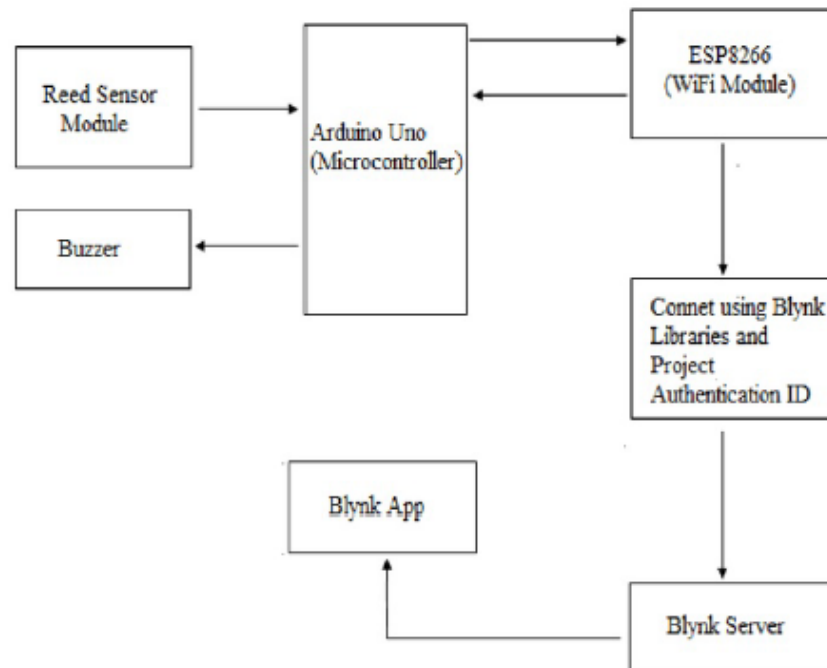
Figure 7. Sketch Diagram.

Figure 8. Architecture diagram of the proposed model.

5. Configuring Blynk App

After the user installs the Blynk app on the smartphone, an account has to be created in the app to access its services. The first time the app is opened, it will ask to either sign in or create an account. Create an account and add a new project to get started as given in figure 9. Each project has its own authentication code which is used by the code to communicate with that particular model as provided in figure 10. To interface with our components, we need to add widgets to our model. To add widgets press '+' to add to the model. The app provides a neat interface to add all the required widgets and setting them up according to the code as shown in figure 11. The Blynk needs to be running in the background for the user to get real time notifications.
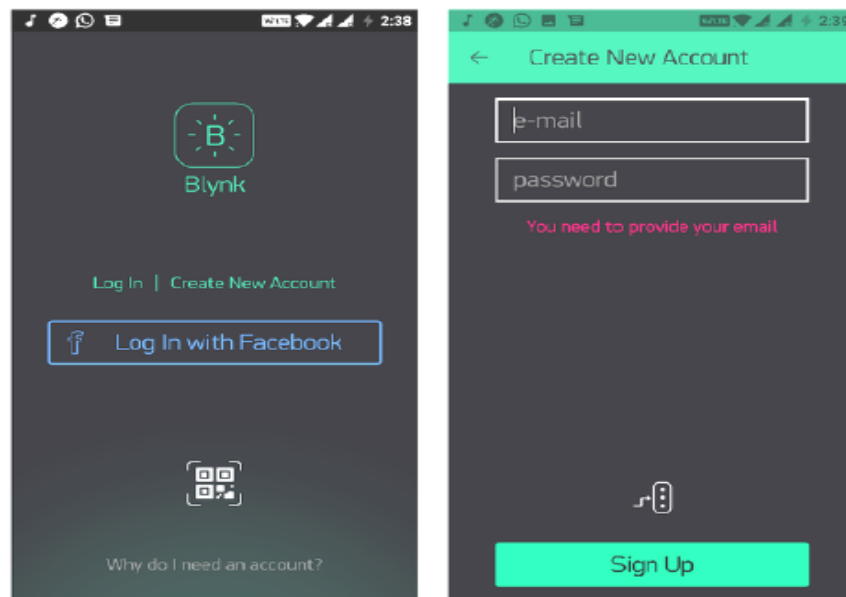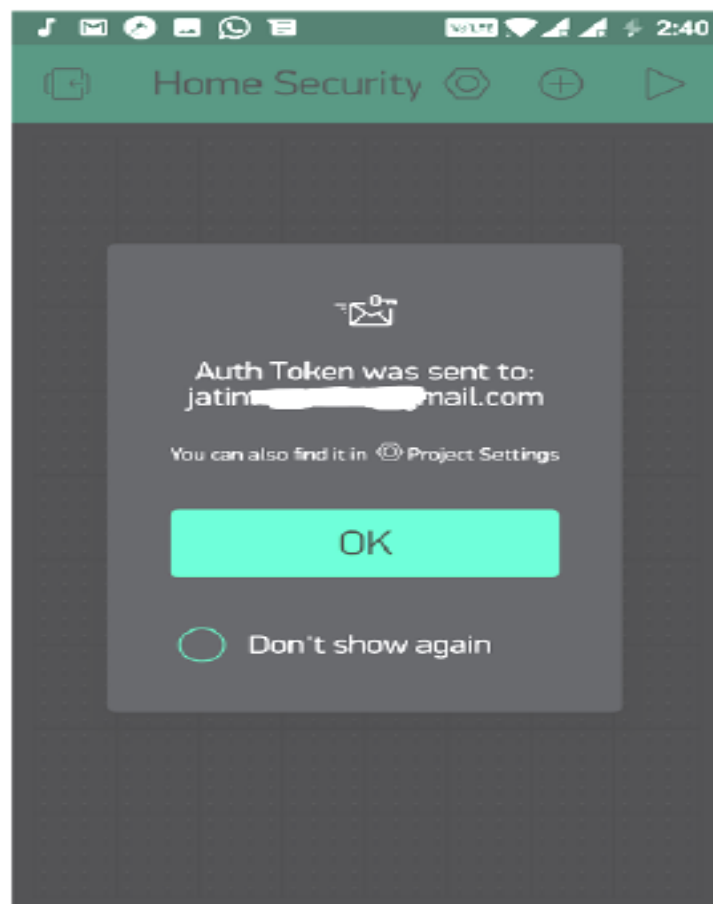
Figure 9. Creating a new account.

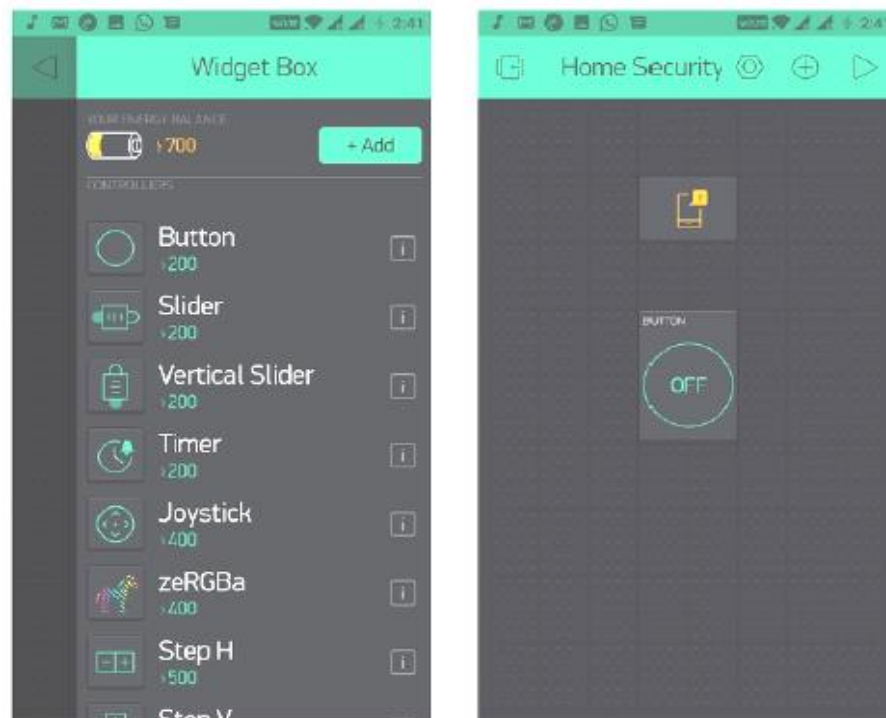
Figure 10. Authentication token.

Figure 11. Adding widgets.

6. Experimental results

The experiment was carried out in Pentium iv 2.60GHz intel dual core processor, with 4 GB RAM, 15' LCD monitor with hard disk as 40 GB. The software required are Blynk App, Arduino IDE, in windows operating system using C++ programming language. The resultant system was checked thoroughly by repeating the motion of opening the door multiple times to see if each time a notification is sent or not and by remotely switching the buzzer on or off from the Blynk app which showed that the system works in the intended way and flawlessly. To test the endurance of the hardware, the setup was left turned on for a couple of hours and tested afterwards. The components got heated which is acceptable but still worked and the notification was shown in figure 12.
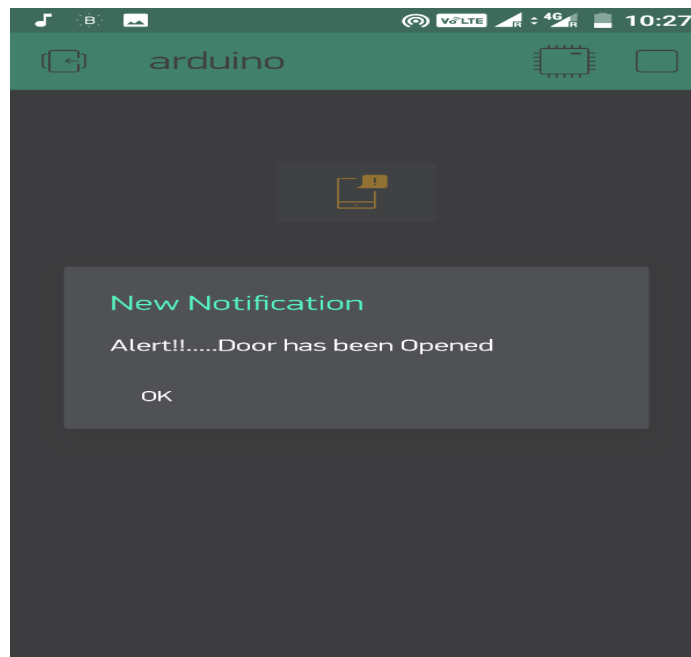
Figure 12. Screenshot of Notification.

7. Conclusion and future scope

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.

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 be disabled for some time so that the user can enter.

References

[1   Govinda K and Sai Krishna Prasad K and Sai ram susheel 2014 Intrusion detection system for smart home using laser rays *International Journal for Scientific Research & Development (IJSRD)* **2** 176-78

[2]   Karri V and Daniel Lim J S 2005 Method and Device to Communicate via SMS after a Security Intrusion *1st International Conf. on Sensing Technology* Palmerston North New Zealand 21-23

[3]   Jayashri B and Arvind S 2013 Design and Implementation of Security for Smart Home based on GSM technology *International Journal of Smart Home* **7** 201-08

[4]   Sowjanya G and Nagaraju S 2016 Design and Implementation Of Door Access Control And Security System Based On Iot *Inventive Computation Technologies (ICICT), International Conference on Inventive*

[5]   Cristian C, Ursache A, Popa D O and Florin Pop 2016 Energy efficiency and robustness for IoT: building a smart home security system *Faculty of Automatic Control and Computers* University Politehnica of Bucharest, Bucharest, Romania 43

[6]   Lee C T, Shen T C, Lee W D and Weng K W 2016 A novel electronic lock using optical Morse code based on the Internet of Things *Proceedings of the IEEE International Conference on Advanced Materials for Science and Engineering* eds. Meen, Prior & Lam

[7]   Pooja P, Mitesh P, Vishwa P and Vinit N 2016 Home Automation Using   Internet of Things *Imperial Journal of Interdisciplinary Research (IJIR)* **2** 648-51

[8]   Anitha A, Paul G and Kumari S 2016 A Cyber defence using Artificial Intelligence *International Journal of Pharmacy and Technology* **8** 25352-57

[9]   Anitha A, Kalra S and Shrivastav 2016 A Cyber defence using artificial home automation system using IoT *International Journal of Pharmacy and Technology* **8** 25358-64