DESK AND CABIN SECURITY SYSTEM

An IoT based Security

[1]Voolla vineeth, [2] Yalamasetty Prasanth, [3]Sadagana Ramu, [4]Kamidi Srinivasu, [5]Sanniti Rama Krishna
[1]UG student, [2]UG student, [3] UG student, [4]UG student, [5]Assistant Professor
[1]Department of Electronics and Communication Engineering
[1]Godavari Institute of Engineering and Technology, Rajamahendravaram, India.

Abstract: This project deals with the design and implementation of Internet of Things based office desk security system. These days all offices are equipped with CCTV camera security system. Even employs seating place is also equipped with CCTV cameras. But shelves of desks used by them are not secure where they keep their important document. So in this project we have concentrate totally on the present generation life style and technologies for getting security to their office desk where generally important document are kept. This project control the devices by using android app just by using internet in there smart phones. The main security is provided by magnetic sensor module which is placed in various shelves of the desk. Whenever desk shelf are tried to open in absence of concerned person then it sends the notification immediately and email to concern persons. Wi-Fi enabled NodeMCU acts like Centralized controller between magnetic sensors and local Wi-Fi router. This router send the information to Blynk cloud and this cloud sends this information to authenticated peered smartphone.

Index Terms – Internet of things (IoT), Magnetic Sensor, PIR Sensor, Blynk App.

I. INTRODUCTION

The internet of things can be described as the technology in which the actual physical entities (electronic devices) with data sensing, processing & self-adoption capacity can be used to interact with other such device and process that data to take an intelligent decision which will prove useful for our daily day to day life. IOT is defined as an environment in which objects (devices) are given unique identifiers and the ability to transfer data over a network without having human-to-human or human-to-computer interaction. The IOT is being formed from two words internet and things which combine means any object or person which can be distinguishable by the real world can be connected to global system of interconnected computer networks and governs by standard protocol. They defined IOT as "An open and comprehensive network of intelligent objects that have the capacity to auto organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" The internet of things is a new era of intelligence computing and it is providing a privilege to communicate around the world. The objective of IOT is anything, anyone, anytime, anyplace, any service and any network.

Imagine an office that automatically opens the door upon your arrival, adjusts the internal temperature by taking cues from the weather outside and sets the electric kettle on the boil for the morning coffee. That is just the bare minimum that Internet of Things (IoT) can help you with at the office.

Workspaces are evolving to incorporate IoT-enabled devices so that almost all aspects of an office space are all data-enabled and driven. This will help cut costs and create more efficient ways in which companies can drive business.

IoT-enabled office spaces would look and 'act' quite differently from the present ones. This means that everything from the furniture to the copier will be connected through IoT.

One of the advantages of an IoT-ready workspace is efficiency. For example, IoT-connected appliances would actively contribute towards cost conservation and optimal utilization of resources, like the LED lights in a meeting room going off as soon as people vacate it. Also, smart devices, with the help of motion sensors, would let employees find a vacant meeting room and locate their co-workers.

Workspaces are evolving to embrace advancements in technology. Organizations are offering their employees means to work smartly with enhanced flexibility and mobility. With the advent of smart devices such as smart phones and tablets, workplaces are witnessing a sea of change in the way of working.

II. METHODOLY

In this project, two magnetic door open sensors have been used and that are placed on two shelves of office desk. These sensors are connected to two pins of the NodeMCU controller and NodeMCU is connected to local Wi-Fi network though on board ESP8266 Wi-Fi shield.

This NodeMCU is connected to IoT Blynk cloud through local wifi and IoT Blynk Cloud is connected to peer smart Phone though authentication key that was generated at time of creation of the project.

For establishing the connection between NodeMCU and local Wi-Fi network, programmer has to provide the Wi-Fi network user name and password in the program that is to be dumped into the NodeMCU.

For establishing the peered communication between NodeMCU and smartphone, generated authentication key is to be mentioned in the program. So whenever Blynk App will be opened, the peer communication will set up through internet.

In this project, we have enabled the Blynk notification and email notification to registered email address and mobile number and one virtual button is assigned on Blynk App to control the operation of the entire system. Whenever user wants to go out then user can enable the system. So user can monitor their valuables even he is not present in office.

In absence of user, if anybody tries to open the shelves then the information of about it will be send to the registered email and mobile number. This system can give instant information to user and user can report to security administration for finding the persons.

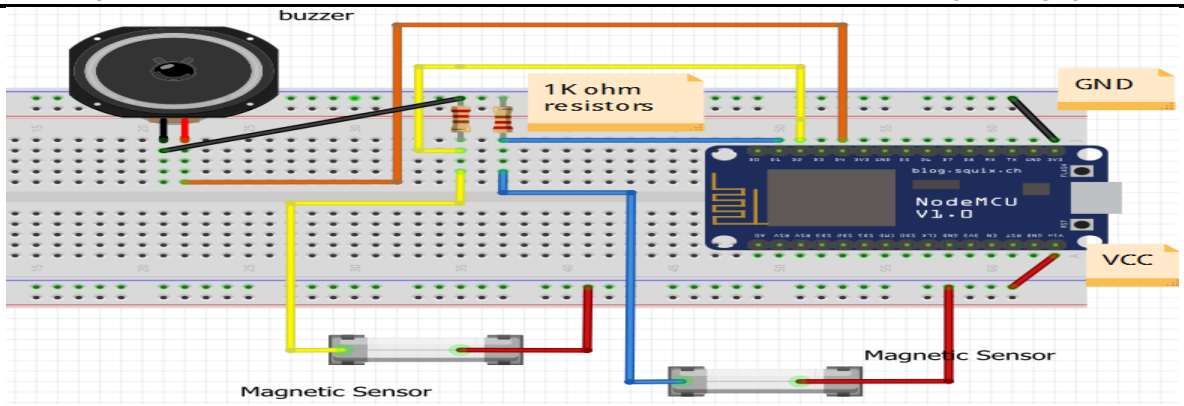

Figure 1: Circuit Diagram

NODEMCU CONFIGURATION:

The NodeMCU (Node Microcontroller Unit) is an open source software and hardware development environment that is built around a very inexpensive System-on-a-Chip (SoC) called the ESP8266. The ESP8266, designed and manufactured by Espressif Systems, contains all crucial elements of the modern computer: central processing unit (CPU), Random access memory (RAM), networking (Wi-Fi), and even a modern operating system and software development kit (SDK).

The most basic way to use the ESP8266 module is to use serial commands, as the chip is basically a Wi-Fi/Serial transceiver. It is recommended to use the very cool Arduino ESP8266 project, which is a modified version of the Arduino integrated development environment (IDE) that you need to install on your computer. This makes it very convenient to use the ESP8266 chip as we will be using the well-known Arduino IDE.

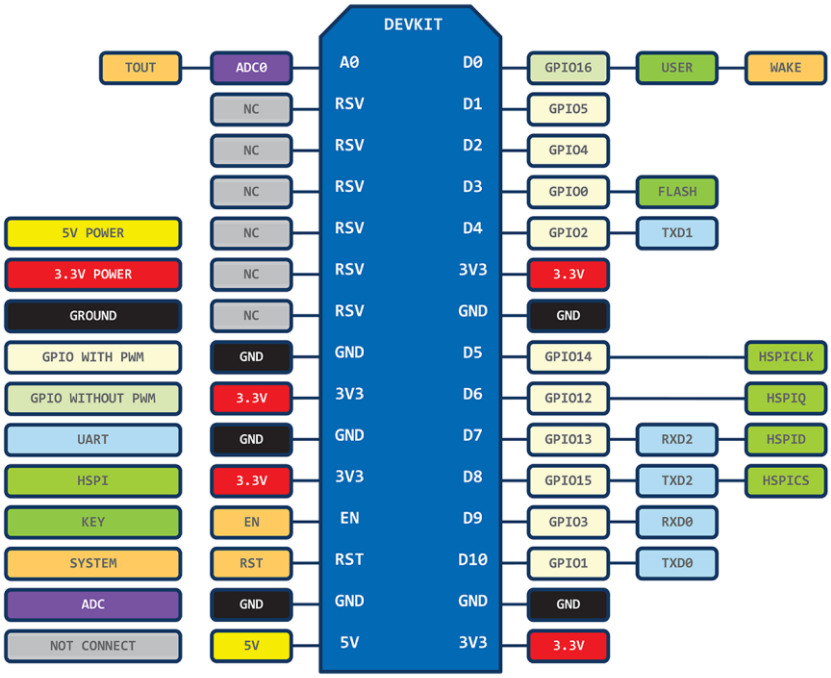

Figure 2: Nodemcu pin details

The above diagram shows the general purpose input-output pins analogous to the digital pins. This helps while configuring the input and output digital pins in the Arduino program. A board that incorporates the ESP8266 chip on a standard circuit board. The board has a built-in USB port that is already wired up with the chip, a hardware reset button, Wi-Fi antenna, LED lights, and standard-sized GPIO (General Purpose Input Output) pins that can plug into a bread board. An open source ESP8266 firmware that is built on top of the chip manufacturer's proprietary SDK. The firmware provides a simple programming environment based on eLua (embedded Lua), which is a very simple and fast scripting language with an established developer community. For new comers, the Lua scripting language is easy to learn.

III. IOT CLOUD ARCHITECTURE

The Internet of Things (IoT) is one of the most exciting and most dynamic areas of Information Technology (IT) at the present time. IoT involves the linking of physical entities (things) with IT systems that derive information about or from those things which can be used to drive a wide variety of applications and services which may be directly or indirectly connected or related to those things. IoT covers a very wide spectrum of applications, spanning enterprises, governments and consumers and represents the integration of systems from traditionally different communities: Information Technology and Operational Technology. As a result, it is important for IoT systems to have architectures, systems principles, and operations that can accommodate the interesting scale, safety, reliability, and privacy requirements.

The cloud components of IoT architecture are positioned within a three-tier architecture pattern comprising edge, platform and enterprise tiers, as described in the Industrial Internet Consortium Reference Architecture. The edge-tier includes Proximity Networks and Public Networks where data is collected from devices and transmitted to devices. Data flows through the IoT gateway or optionally directly from/to the device then through edge services into the cloud provider via IoT transformation and connectivity.

The Platform tier is the provider cloud, which receives, processes and analyzes data flows from the edge tier and provides API Management and Visualization. It provides the capability to initiate control commands from the enterprise network to the public network as well. The Enterprise tier is represented by the Enterprise Network comprised of Enterprise Data, Enterprise User Directory, and Enterprise Applications. The data flow to and from the enterprise network takes place via a Transformation and Connectivity component. The data collected from structured and non-structured data sources, including real-time data from stream computing, can be stored in the enterprise data.

IOT gateway acts as a means for connecting one or more devices to the public network (typically the Internet). It is commonly the case that devices have limited network connectivity – they may not be able to connect directly to the Internet. This can be for a number of reasons, including the limitation of power on the device, which can restrict the device to using a low-power local network. The local network enables the devices to communicate with a local IoT Gateway, which is then able to communicate with the public network. The IoT Gateway often has other capabilities, including the ability to filter and intelligently react to data, the ability to send and receive data or commands to and from the Internet, the ability to run application or service logic locally (processing data and executing control logic without the need to communicate to a central location). It can also provide operational efficiency by allowing multiple devices to share a common connection.

A cloud computing environment provides scalability and elasticity to cope with varying data volume, velocity and related processing requirements. Experimentation and iteration using different cloud service configurations is a good way to evolve the IoT system, without upfront capital investment. It provides core IoT applications and associated services including storage of device data, analytics, process management for the IoT system, creates visualizations of data and also hosts components for device management including a device registry.

IV. BLYNK CONFIGURATION

Blynk was designed for the Internet of Things. It can control hardware remotely, it can display sensor data, it can store data, visualize it and do many other cool things.

There are three major components in the platform:

Blynk Application –It allows to you create amazing interfaces for your projects using various widgets we provide.

Blynk Server –This is responsible for all the communications between the smartphone and hardware. You can use our Blynk Cloud or run your private Blynk server locally. Its open-source, could easily handle thousands of devices and can even be launched on a Raspberry Pi.

Blynk Libraries –It is for all the popular hardware platforms - enable communication with the server and process all the incoming and out coming commands.

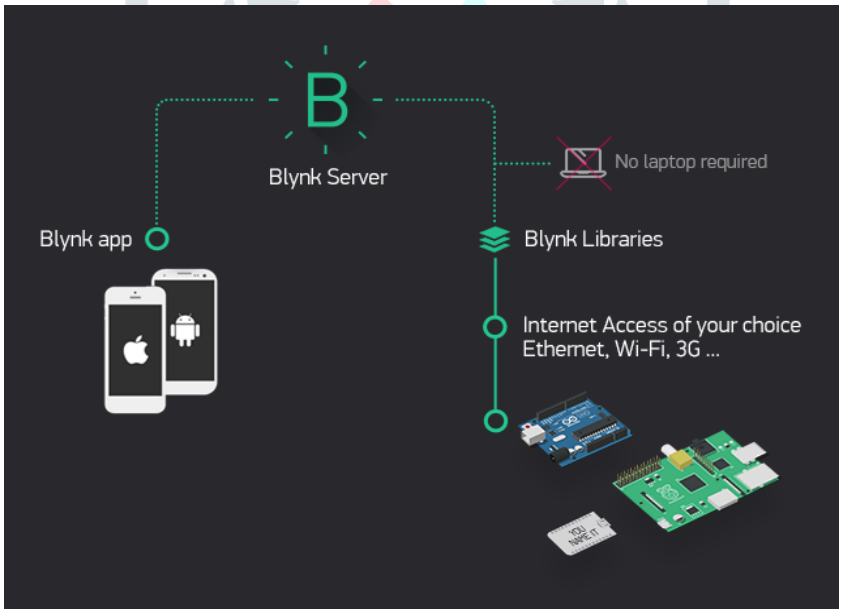

Figure 3: Blynk cloud architecture

BLYNK WIDGETS:

Widgets are interface modules. Each of them performs a specific input/ output function when communicating with the hardware. There are 4 types of Widgets:

- **Controllers** - they send commands to hardware. Use them to control your stuff
- **Displays** - used for various visualizations of data that comes from hardware to the smartphone
- **Notifications** - are various widgets to send messages and notifications
- **Interface** - are various widgets to make your UI look better
- **Others** - widgets that don't belong to any category

Each widget has its own settings. Some of the Widgets (e.g. Bridge Widget) are used to enable some functionality and they don't have any settings.

AUTHENTICATION TOKEN:

Authentication token is a unique identifier which is needed to connect your hardware to your smartphone. Every new project you create will have its own authentication token. You'll get authentication token automatically on your email after project creation. It's very convenient to send it over e-mail. Press the e-mail button and the token will be sent to the e-mail address you used for registration. You can also tap on the Token line and it will be copied to the clipboard.

V. RESULT

We get notification like this in the blynk app when some entered and open the desk in the cabin.

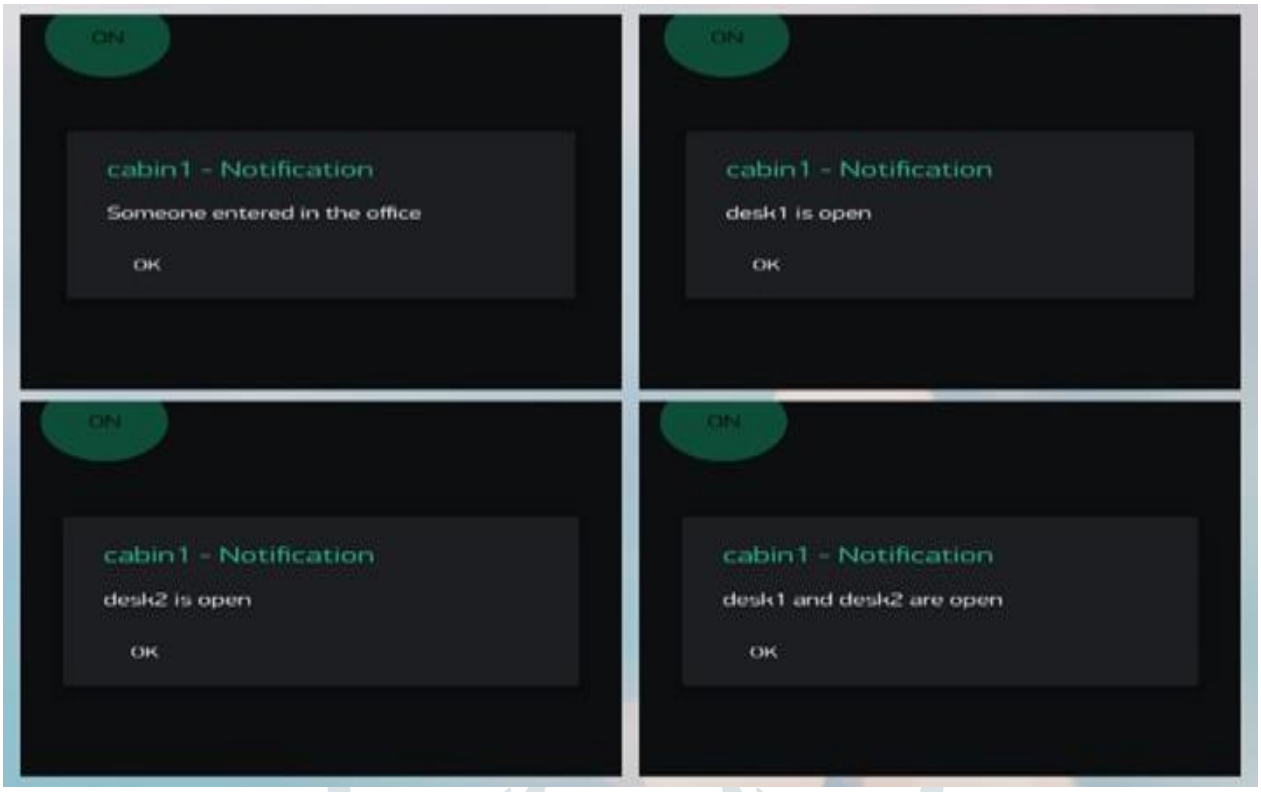

Figure 4: Screenshots of Notification

VI. 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 Buchares.