TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

INTEGRATIONOF IFTTT AND ONLINE VOICE BASED SECURITY SYSTEM FOR REAL TIME APPLICATION USING IOT

M.Natarajan[1], A.Dhivya[2], A.FlorinSona[3],S.Harishma[4], T.Kawsalya[5]

[1,2,3,4,5] Department of Computer Science and Engineering, K. Ramakrishnan College of Technology, Anna University, Trichy

[1]forevernatarajan@gmail.com, [2]dhivyaaynan10@gmail.com, [3]florinsona99@gmail.com, [4]harishmasara@gmail.com, [5]kawsy1305@gmail.com

Article Info
Volume 82
Page Number: 9410 - 9419
Publication Issue:
May - June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *18 May 2020*

Abstract

Nowadays, Security system could be a major concern everywhere. Most of the safety systems have various loopholes to access data from the required place of environment. This paper portrays to style an occasional cost-effective voice based security with the utilization of an integrated Arduino and wireless protocol connectivity for access and to manage of bank locker and plenty of real time applications remotely by the usage of android based smartphone IOT app. The system is implemented using ordinary tongue voice commands. These commands are given to the Google Assistant with the assistance of IFTTT(IF THIS THEN THAT) application and BLYNK application. Now the commands are decoded and sent to the microcontroller, the microcontroller successively controls the relays connected to that. Turning the device connected to the respective relay ON or OFF as per user request to Google Assistant. additionally, to the present RFID tag is employed for providing otherwise of security to the locker systems.

Keywords; *Voice based security, IFTTT, BLYNK, RfID.*

1.INTRODUCTION

In today's busy and competitive world security is of primary concern and human cannot find ways to produce security to their data. During this ubiquitous society, where individuals can effortlessly access their information anytime and anywhere. People also are endured with the chance that others can even access the data from anywhere at any time. Because of this risk, personal identification technology is employed that distinguishes between registered legitimate users and illegitimate users.

Internet of Things is connecting one device to a different device via internet. The physical devices around us are connected using sensors, and chips. Each device has their data. Each device is assigned with their unique identifiers(UIDs). Now diverse of knowledge is retrieved from different physical device by securely communicating using internet of things platforms. Now, this platform is emerging in all the industries possible like agriculture, transportation and so on. The important thing to be noticed is that only the machines are communicating between themselves no human interruption is present. The human interruption is present only for setting up and accessing of data.

Currently, passwords, personal identification numbers or cards are used for private identification. However, cards may be embezzled and passwords may be speculated. Within the present day scenario the locking system hold keys. The existing system also includes biometric system. This biometric system includes face recognition, finger print and iris recognition. The biometric system has major

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

advantage that the owner can be identified specifically but this turns out to be a disadvantage because only the owner can access the locker. Even in case of emergencies the owner's relatives or guardians cannot open the locker. In the proposed system this disadvantage is rectified.

Since 2000 years ago, we've got been using lock and key. The locking system is prerequisite for all. The locking system are traditionally the mechanical locks that use keys. Such styles of systems are vulnerable in various ways by flawing security. It's observed that bank lockers, bungalows, houses, shops and repositories in security aspect ends up in loss of sensitive and guidance. The standard locking system does'nt seem to be adequate to diagnose any pirated access, security breach and does'nt provide solid authentication policy.

In recent times, technology is developed with the enhancement of the Internet and also, we had moved to wireless communication for locking system. Keypad electronic locking system is prominent. During this keypad locking system, we'd like not need any keys because we use passwords for locking system. But it's many detriments like forgetting the password, hacking of password, unable to open the door just in case of power outage. To reinforce security and authentication, electronic locking systems are devised. Encrypted and secure lock system may be connected to GSM and Bluetooth.

The mobile software system and internal applications, we are able to remotely supervise voice locking system for bank and plenty of other real time applications. IFTTT could be a web service smart app running on smart things as an agent and IFTTT server access the devices in smart things. IFTTT can even join various Internet services like Facebook, Instagram, Gmail etc. Blynk could be a platform with android apps to manage Arduino over the web.

The microcontroller used is Node MCU (ESP8266). The communication between microcontroller and therefore the application is established via Wi-Fi (Internet) . Hence, the digitalized smart security system could be a unique combination indulging absolute solution for various aforesaid security measures for the matter of security

II. RELATED WORKS

In this proposed system, the voice recognition is done using google assistant and the connection between the devices and google assistants done using ITFFF.

Digital door locking system was implemented using zigbee and it is operated by digital key and security password. It was mainly focused on making the digital door lock a consumer device. This system was implemented by H-kyu Hwang.[1]

Phone based remote control system for controlling home and office automation was implemented by IsmailCoskun.[2]

By using IOT real time monitoring, remote control, safety from intruders for smart home was proposed by Zaied Shouran.[3] Since IOT has been used, devices become ubiquitous and contribute to the broader understanding of user's evolving attitudes towards privacy.

IOT is used for saving electricity bills and control switches can be remotely accessed and monitored with or without an android based app. This concept was implemented by Jasmeet Chhabra.[4]

Authentication provided for user from malicious readers by using RfID tag which was proposed by Divyan M. Konidala.[5] Therefore RfID provides security for home appliances that requires security.

Controlling of lock using mobile app via Bluetooth which was proposed by Varad Pandit.[6] The mobile app is used for face recognition of the owner that is used to control the locker system.

Advait churi proposed digital interface for the user to access the locker along with the feature that the administrator is sent a mail notification and captured

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

image of the user.[7] The password entered by the user using bluetooth connected smart phone.

WiFi based development, remotely monitor the conditions within home and control the home appliances was proposed by Ravi Kishore Kodali. Sensors and actuators are connected to ESP8266. A mosquito based MQTT broker is established for remote monitoring and control.MQTT is a light weight protocol that consumes less energy and occupies low bandwidth.[8]

By using android based smart phone app Nathan David proposed a system to control home appliances. The smart home system is designed and created by WLAN network based on Arduino microcontroller.[9]

Complete biometric based authentication for locker system was proposed by Srivatsan.[10].

By using IoT various devices are connected for developing a smart home using multiple language voice commands via Google assistant to control home appliances and smart door unlocking system. This system was proposed by Vivek Raj.[11]

To improve home security Arun Cyril proposed that by using combination of sensors, controllers, Raspberry PI and ZigBee communication to identify user behavior at various points and implement logical sense algorithm.[12]

Energy saving for electrical appliances is done using IOT. In small areas it is done by connecting all the appliances to a common WiFi network. This system was proposed by Alok Kumar Gupta.[13]

The secured lock system is provided by using Bluetooth technology. Since, it is available in almost all the gadgets and low cost. This system was proposed by Muhammad Sabirin Hadis.[14]

III.EXISTING SYSTEM

A. KEY BASED SYSTEM

The key based security is the first security system used initially to provide security for locker based system. This system contains a lock for each locker and appropriate keys will be provided.

B. KEYPAD BASED SYSTEM

The keypad consists of a specific number if digit or alphanumeric code. This can be set by the owner of the data. But the disadvantage of this system is that the password can be forgotten by the owner or the passcode can be leaked to the third person and it also does’nt support in emergency situation if the passcode is not known other than the owner.

C. BIOMETRIC BASED SYSTEM

The biometric based system includes finger print, iris, retina and so on.

C.1. FINGER PRINT

The unique finger impression based bank storage framework is an improvement to the conventional bank storage framework that utilizations keys. Presently keys can without much of a stretch be duplicated and made by theif's who think about it. Likewise the keys must be dealt with and can likewise be lost because of some carelessness. Well unique finger impression based bank storage framework is here to unravel every one of these issues. The fingerprinted validated bank storage framework is sheltered just as simple to utilize and keep up**.**

C.2 IRIS BASED SYSTEM

This is a unique way of identifying the person. The disadvantage of finger print based system is that in this type of system cloning can be performed by the third person. But this system also has a disadvantage that even in an emergency situation no third person can access the system.

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

IV .PROPOSED SYSTEM

The proposed system is to design secure locker using voice based security and RFID tag. The natural language voice commands are given to Google Assistant using IFTTT and Blynk application.

The domain focused here is IOT which involves the computing devices that are provided with unique identifiers and ability to transfer data without involving human – human or computer – human interaction.

A .ARCHITECTURE

The architecture diagram involves the voice based security system(FIG. 1). This system works by mailing the voice password to the micro controller device using the mobile application. This mobile app is connected to the Arduino device via Wi-Fii. The facility supply are going to behanded right down to the Arduino device which collocate and inscribe the password. Google assistant is employed to acquaint information about the status of the password.

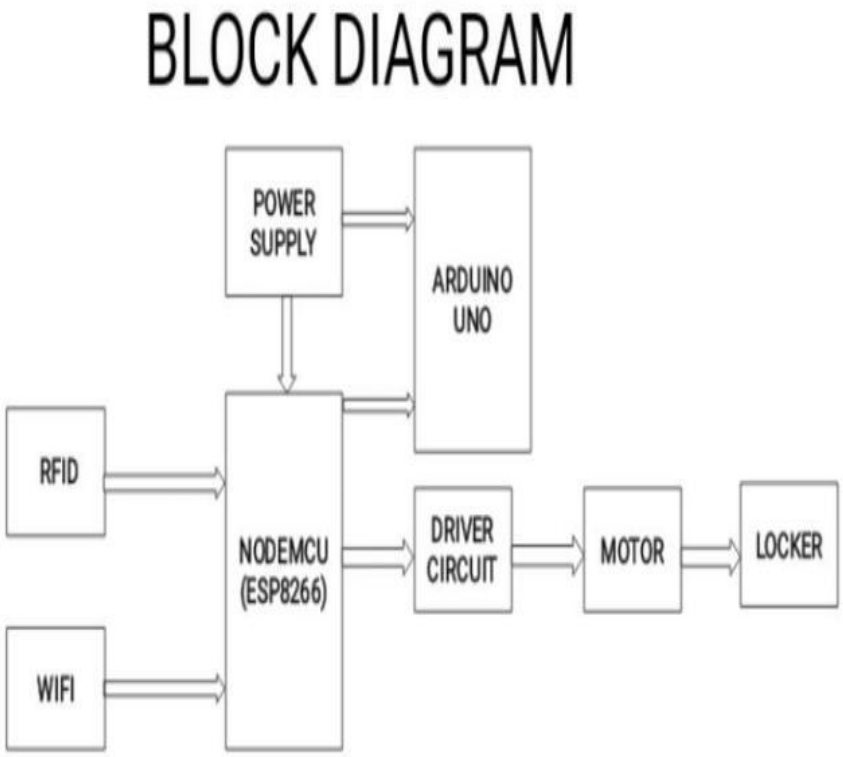

Fig. 1

The Arduino device where the password is already programmed in it compares the given signal with the stored signal. Relay driver circuit is employed to lock/unlock the bank locker. If the password is matched the lock are going to be susceptible, otherwise the status message are going to be circulated to the authenticated person's mobile number using IOT module and therefore, the lock remains within the same state using IOT.

A.1.SYSTEM DESIGN

The system design is divided into two main categories,

>Hardware

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

>Software

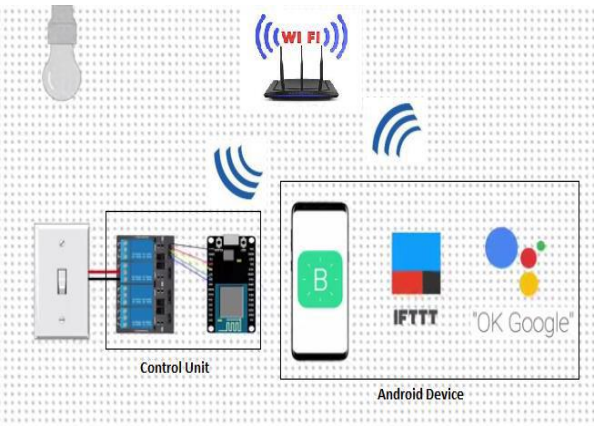

Fig.2

HARDWARE- It has the aptitude to attach to the router. It might even be ready to turn on/off specified devices. It is called as the "Control Unit". The hardware also consists of power supply unit.

The Control Unit comprises the microcontroller Node MCUU) and therefore, the 4/8 Channel Relay board. Relay board uses ULN 2803 IC to manage the relays.

SOFTWARE- The Blynk app, the IFTTT app and therefore,e, the Google Assistant constitute the software of the planning, and these applications would be integrated within the Android device.

The Blynk app on an Android device communicates with the microcontroller and sends the specified signal via the net. If This Then That, also called IFTTT, is employed to attach different apps and devices.

B.DETAILED PROCESS

B.1.RFID TAG-

Radio Frequency Identification Tag(RFID) is an electronic tag that exchanges data with the reader module through radio waves. RFID is employed as wireless communication that contains the utilization of electromagnetic coupling within the frequency partto uniquely identify anything.

So Basically, there are two varieties of RFID. They are active and passive RFID. The active RFID has its own battery. Whereas, passive RFID does'nt, receive power from batteries rather it receives power from the reading antenna. In our system, passive RFID is being employed. RFID tag stores only less amounted of knowledge that's but 2000 KB.

Fig.3

The 

RFID consists of three major components. They are scanning antenna, receiver and transponder. When this scanning antenna and transponder is combined then it's the RFID reader. The reader is network connected device. The reader is portable or it may be permanently attached.

Thus, tagging items with RFID tags allows users to automatically and uniquely identify and track the assets. RFID may be read within few centimeters. The RFID tag is read by the EM 18 reader Module.

A radio frequency identification reader(RFID peruser) is a gadget used to assemble data from a RFID tag. Radio waves are utilized to move information from the tag to a peruser. RFID is an innovation comparable in principle to scanner tags. In any case, the RFID tag doesn't need to be examined straightforwardly, nor does it require view to a peruser.

The RFID label it must be inside the scope of a RFID peruser, which ranges from 3 to 300 feet, so as to be perused. RFID labels have not supplanted standardized tags in view of their expense and the need to separately recognize each thing.

B.2.ESP8266-

It is an occasional cost Wi-Fi module which is employed for interfacing for microprocessors. The

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

ESP8266 features a 64 KIB of instruction RAM and 96 KiB of knowledge RAM.

The board may be powered from two voltage sources. High voltage to the HV pin, Low voltage to the LV pin and ground from the system to GND pin.

The ESP8266 is able to do either facilitating an application or offloading all Wi-Fi organizing capacities from another application processor. Each ESP8266 module comes pre-programmed with an AT command set firmware, which means, you can essentially connect this to your Arduino gadget and get about as much WiFi-capacity as a WiFi Shield offers.

It is accustomed check whether the recognized password is correct or not. The password is verified with the first password stored within the database. According to the verification, the legal and Illegal user may be found.

B.3.ARDUINO UNO-

It is the foremost popular microcontroller within the industry. It is user convenient and easier to handle. The coding or programming of this controller is additionally easy and therefore, the program is deemed thanks to the volatile and non-volatile storage. The device has the aptitude to be connected and act as a server too.

Arduino UNO consists of the USB interface, digital I/O pins (14 pins), analog pins (6 pins), and Atmega328 microcontroller. Arduino Uno supports serial communicatio , and it contains RX and TX pins. This contains all the necessary help required for microcontroller. So as to begin, they are just associated with a PC with a USB link or with an AC-to-DC connector. Arduino Uno Board shifts from every single other board and they won't utilize the FTDI USB-to-sequential driver chip in them. It is highlighted by the Atmega16U2 (Atmega8U2 up to adaptation R2) customized as a USB-to-sequential converter.

When Arduino UNO must be programmed and it's done by connecting the laptop/computer using USB cable. This suggests that additionally the Arduino UNO needn't be powered while programming. It may be powered up with the pin within the header.

B.4.ANDROID DEVICE-

The android device consists of two applications to connect to the locker. They are,

- BLYNK application
- IFTTT application
- Google Assistant application

BLYNK-

Blynk could be a platform with IOS and android apps to manage Arduino. Blynk is one amongst the foremost user-friendly and it’s also free and open-source. With Blynk, though, the software side is even easier than the hardware.Blynk are often accustomed to create an area Blynk server, allows to stay everything within your own residence network. Blynk is ideal for interfacing with simple projects like monitoring the temperature or turning lights on and off remotely.

It is a digital dashboard which is employed to make a graphic interface for the project by simply dragging and dropping readily available widgets.Using the widgets, you'll be able to turn pins on and off or display data from sensors. Therefore, the BLYNK application is employed as an graphic interface for this project.

IFTTT-

IFTTT is acronymed as If This Then That, which could be a free web-based service that makes simple applets. Applets are specific things that can happen when you connect services.It creates simple chains of conditional statements. Widgets are shortcuts that allow to run certain Applets with the touch of a button on your iOS or Android device.

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

To use applets, we must have the IFTTT app on the phone. After turn on a widget Applet, we can add it as an icon in the home screen on iOS or Android.IFTTT is employed as a macro that connect different apps to perform automated task. IFTTT is employed to attach Google assistant. In order that the password may be recognised by the Google assistant and can initiate the locker to beopened.

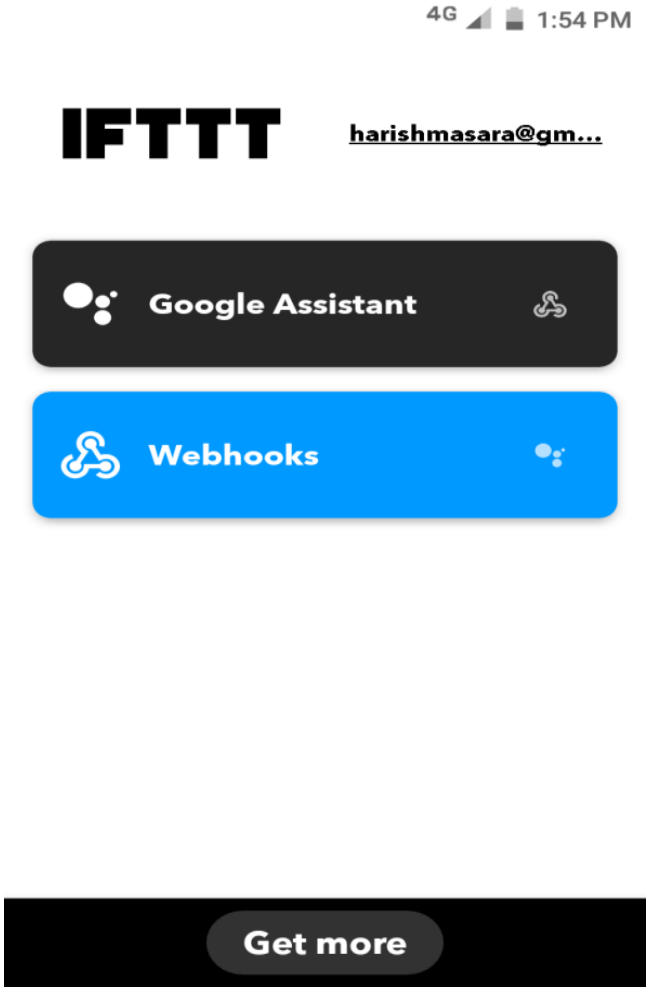

Fig.4

By using IFTTT app, google assistant is connected and therefore, the password is recognized through google assistant which stimulates the locker to open.

Additional level security is provided by using RFID tag. Double layer security is provided in this paper. The same process is done for closing the locker. The close command that is already set is spoken to the google assistant. This natural language voice command is recognised and which initiates the locker to be closed.

B.5.LOCKER-

The system is implemented by giving ordinary Natural language voice commands Google Assistant and with the help of IFTTT (If This Then That) application and the Blynk application the commands are decoded and then sent to the microcontroller, the microcontroller in turn controls the relays connected to it as required, turning the device connected to the respective relay On or OFF as per the users request to the Google Assistant.

V.OUTPUT

The below hardware kit consists of the following,

Published by: The Mattingley Publishing Co., Inc.

1. Power supply unit
2. ESP8266
3. EM 18 Reader Module
4. ARDUINO UNO
5. Relay Module
6. Motor

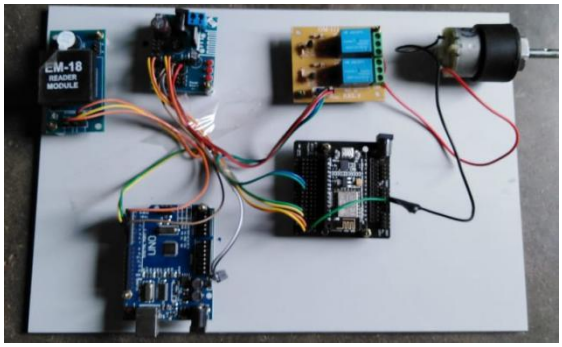

Fig.5

The output that is obtained from Google Assistant using IFTTT application is given below,

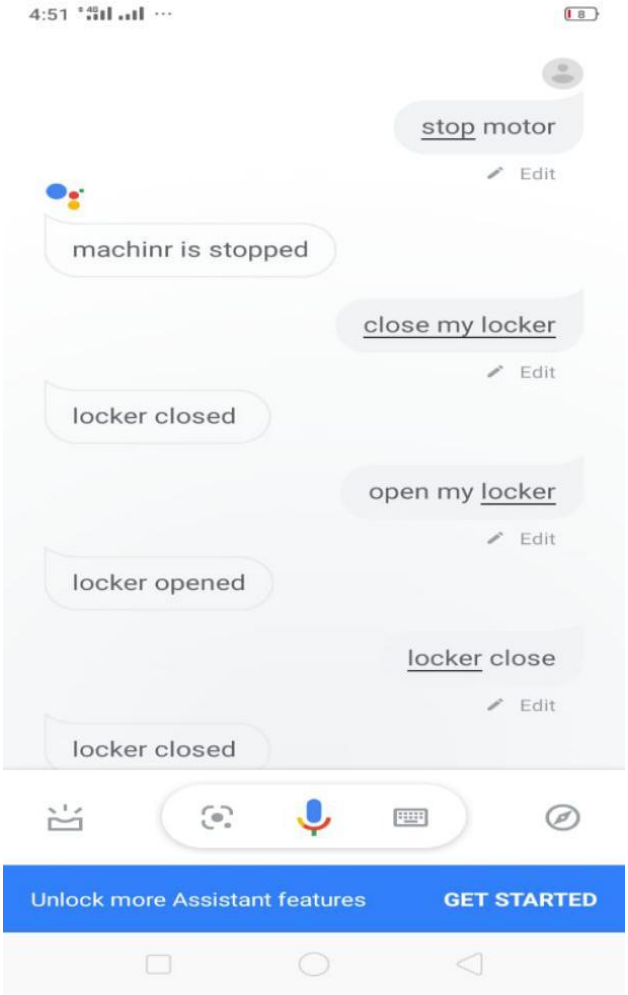

Fig.6.RESULT

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

If the command to open the locker is given in Google Assistant then it will make the locker to open. The same procedure will be followed for closing the locker. Then if the locker is opened or closed the suitable result will be provided in the google assistant. We can set upto three passwords for open and closing of the locker. For instance, in Fig.6 for "open my locker command" the locker will be opened and the reply will be "locker opened". This can also be set by the owner. Then if "locker close" is said then the reply will be "locker closed" and the locker will also get closed.

VI.CONCLUSION

As security is a major concern these days, thus by using the simple voice recognition is used to provide security for real time applications using IFTTT. In others words, simple voice based security for locker based system is implemented in this paper. The system provides security by additionally using RfID tag that makes the system more reliable. This paper provides double layer security for the real time apllications. This system provides 97% of overall accuracy.

VII.REFERENCES

[1] Il-kyu Hwang and Jin-Wook Baek proposed Wireless access monitoring and control system based on digital door lock, 2007.

[2] Ismail Coskun and H Ardam proposed A remote controller for home and office appliances by telephone, 1998.

[3] ZaiedShouran, Ahmad Ashari and Tri Kuntoro Priyambodo proposed Internet of Things(IoT) of smart home : Privacy and Security, 2019.

[4] Jasmeet Chhabra and Punit Gupta proposed IoT based Smart Home design using power and security management, 2016.

[5] Divyan M. konidala, Daeyoung Kim, Chan Yeob Yeun and Byoungcheon Lee proposed Security Framework for RFID- based Applications in Smart Home Environment, 2011.

[6] Varad Pandit, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga and Sachin Bojewar proposed Intelligent security lock, 2017.

[7] Advait Churi, Anirudh Bhat, Ruchir Mohite and Prathamesh P.Churi proposed E-Zip: An electronic lock for secured system, 2016.

[8] Ravi Kishore Kodali and SreeRamya Soratkal proposed MQTT based home automation system using ESP8266, 2016.

[9] Nathan David, Abafor Chima, Aronu Ugochukwu and Edoga Obinna proposed Design of Home Automation System using Arduino, 2015.

[10] Srivatsan Sridharan proposed Authenticated secure biometric based access to the bank safety lockers, 2014.

[11] Vivek Raj, Athul Chandran BS and Anu Prabha RS proposed IoT Based Smart Home Using Multiple Language Voice Commands, 2019.

[12] Arun Cyril Jose and Reza Malekian proposed Improving Smart Home Security : Integrating Logical Sensing Into Smart Home, 2017.

[13] Alok Kumar Gupta and Rahul Johari proposed IoT based Electrical Device Surveillance and Control System, 2019.

[14] Muhammad Sabirin Hadis, Elyas Palantei, Amil Ahmad Ilham and Akbar Hendra proposed Design of smart lock system for doors with special features using bluetooth technology.

[15] T.Ciardiello proposed Wirelesscommunications for industrial control and monitoring,2005.

[16] K.Sangani proposed Home automation - It's no place like home, 2006.

[17] N. Baker proposed Bluetooth strengths and weaknesses for industrial applications, 2006.

[18] T. B. Zahariadis and A. K. Sakintzis proposed Introduction to special feature on wireless home networks, 2003.

[19] Sandeep Patel, Punit Gupta and Mayank Kumar Goyal proposed Low Cost Hardware

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 9410-9419

Design of a Web Server for Home Automation Systems, 2013.

[20] A.Z. Alkar, Univ Hacettepe, J. Roach and D. Baysal proposed IP based home automation system, 2010.

Published by: The Mattingley Publishing Co., Inc.