Smart Secure Home Automation

1Sanjeev Kumar, 2Avneet Kaur Batra, 3Aishwarya, 4Devraj Gautam
1Student, 2Student, 3Student, 4Assistant Professor
Dr. Akhilesh Das Gupta Institute of Technology & Management

***Abstract* - Security issue is one of the major concerns in our society these days. Keeping that in mind, this paper provides maximum possible security required in the hardware system. Security components as of the MAC filter, i.e. the hardware security, biometric security and many more are listed in this paper along with a brief description and implementation demo. The technology as well as the prototype designed and implemented can be used for application in offices, houses, even in the military truck for loading the assets as the designed system is a multipurpose Smart and Secure Automated system. In case of a security loophole, many ways are provided to report the issue and problem to the concerned authority or personnel. The Application for system prototype is designed using MIT App Inventor and sensors are connected to the Application using Google Firebase via bucket token authentication.**

I. INTRODUCTION

In this current time, incidents as robbery, stealing, unwanted entrances are happening frequently. So the security matters most in daily life. As people remain busy in their day to day life and work they want ensured safety of their beloved ones and possessions. Most often people misplace their necessary things like keys, wallet, credit cards etc., because of which they unable to access their home or any place they want to get in. Traditional security system require a user key, a security password, a RFID card, or ID card to have access to the system. However, these security systems have deficiencies; for example, they can be forgotten or stolen from unauthorized people. As a result, there is a need to develop intelligent system that guarantees a higher security level is a template. One of the unique features of our brain is that it can think only in images not in words. There is a quite possibility to lose a key but unlikely to be denied access by use of face or fingerprint.

From a long year ago, we are using non-living thing (smart cards, plastic cards, PINS, tokens, keys) for authentication and to get grant access in restricted areas like ISRO, DRDO etc. There are two types of biometric as physiological characteristics (face, fingerprint, finger geometry, hand geometry, palm, iris, ear and voice) and behavioural characteristics (gait, signature and keystroke dynamics). Sometimes your behavioural traits may changes because of illness, fear, hunger etc. Face and finger print detection and recognition system is more cheap, simple, accurate and non-intrusive process as compare to other biometrics. The system will fall into two categories as fingerprint detection (1:1) and fingerprint recognition(1:N).In the fingerprint detection we have to classify between fingerprint versus non fingerprint region while in recognition process we have to compare that single fingerprint image with the image stored in database of your security system app.

We have used an amalgamation of various sensors so as to automate the lighting system. When someone enters the house, the motion sensor will detect it and switch on the lights in the areas when and where it is required. When the sun sets, the LDR will switch it on. Fire sensor will send in the notification to our phone in case there is fire anywhere in the house.

II. RELATED WORKS

Today, people are facing more problems about security in all over world, nowadays security is the most essential issue everywhere in the world; so security of everything gains higher and higher importance in recent years. We are trying to produce a comprehensive literature study related to various door locks and gate security systems necessary in the fields of home, industries and vehicle security where possibilities of incursion are increasing day by day.

In past days, the research is gone on various door lock security systems like traditional security systems which provide indications using alarm. Due to the advancement in recent techniques, some door lock security systems are based on microcontroller, GSM, GPS, many sensor software like MATLAB, PROTEUS, and biometrics like face recognition, iris scanner, RFID, Smart Card and password etc. Each system has its own advantages and disadvantages. In most systems, SMS technique is used for communication so that the system becomes cost effective, more reliable and it will take less time to deliver message. As security becomes major problem nowadays, the security monitoring systems today need to make use of the latest technology. In some papers, the authors have presented door lock security monitoring system based on embedded and Zigbee where the lock is protected by automatic password hence it could not easily hack by hackers. Also the enhanced security systems are available based on android platform, wireless techniques and embedded systems. A lot of modification takes places in various Door lock security from the last few years, in next coming years many changes will takes place.

Security has always been a concern of paramount importance to human beings. We have gone from protecting valuables in the past, keeping them in dungeons to safeguard our data by layers and layers of cryptographic software. Either way, ensuring the well-being of our personal belongings has always been near the top priority. Our home is the best place where we keep our personal belongings. What about the security of our home? There is no doubt that our door locks play a major role in keeping our home safe.

Biometric door locks are now common with increased security levels and ensure the protection of our door locks. But there are two things that prevent the use of biometric locks. One is the cost of the lock starting from $300 and other is the lack of remote access. So let's add some IOT flavour to make the biometric door lock spicier.

III. TECHNOLOGY IMPLEMENTED

FRAMEWORK DIAGRAM

- This system requires a NodeMCU (ESP8266), which acts as controller and server of the whole system.
- Before door opening, this system requires user identification i.e. the finger print detection and recognition.
- The finger print detection and recognition is done by using an application in smart phone with user login.
- After successfully recognized the user, application program will send an authentication to NodeMCU to unlock the door.

After which we enter the house and can use automatic lights and other features.
We can operate these features via an app or via Google assistant.
We have connected these together individually in different parts of the house hence we have 3 distinct circuit diagrams as follows:

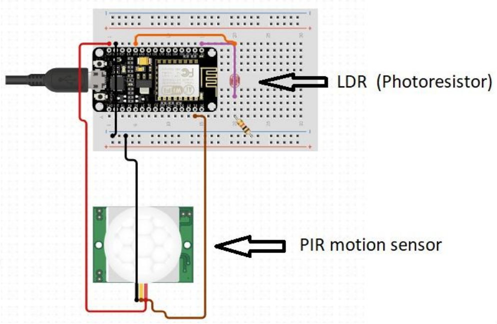


Fig.1: Circuit Diagram for PIR Motion Sensor with ESP8266

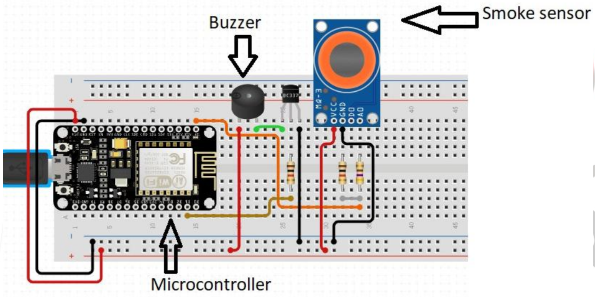


Fig. 2: Circuit Diagram for Smoke Sensor with ESP8266

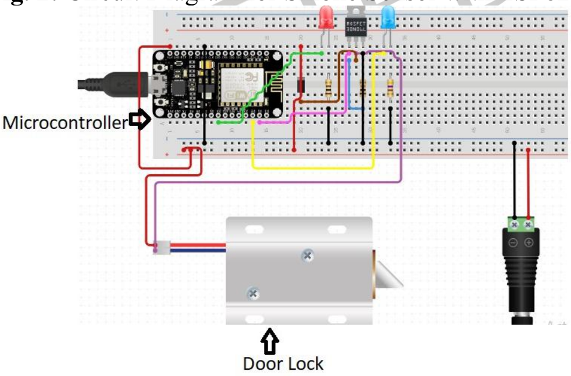


Fig. 3: Circuit Diagram for Door Lock with ESP8266

So to ensure the security and remote access we want to think of a new way to connect our door lock to our personal devices. Let's think about our mobile phones, they have the capability to control our smart door locks through MQTT and available protocols. Then why don't we add an additional biometric firewall to that? Yeah, that's what we are gone do. Nowadays almost all mobile phones are equipped with fingerprint sensors. We use them to verify the biometric of the authorized person. So it can overcome the disadvantages of now existing smart door locks with an increased security level. In essence, we are going to build a Smart Remote door lock with additional biometric security. As almost all smart phones are equipped with fingerprint sensors and we are using those sensors to verify the identity. The data read from the fingerprint sensor is compared with the authentic fingerprints stored in the device using a mobile application and determines whether the person is authorized or not. The data after verification is sent from mobile to a suitable cloud database, from where the smart door lock system retrieves the data. If the person authorized the smart door lock will unlock and if the person is not authorized it doesn't unlock.

We have used an amalgamation of various sensors so as to automate the lighting system. When someone enters the house, the motion sensor will detect it and switch on the lights in the areas when and where it is required. When the sun sets, the LDR will switch it on. Fire sensor will send in the notification to our phone in case there is fire anywhere in the house. It works with Google Assistant.

VI. HARDWARE

NodeMCU ESP8266

NodeMCU is an open source IOT platform. It includes firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module. The term "NodeMCU" by default refers to the firmware rather than the development kits. The firmware uses the Lua scripting language. It is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266.

NodeMCU Kit has Arduino like Analog (i.e. A0) and Digital (D0-D8) pins on its board. It supports serial communication protocols i.e. UART, SPI, I2C etc. NodeMCU Development board is featured with wifi capability, analog pin, digital pins and serial communication protocols.

- Easy to program wireless node and/or access point
- Based on Lua 5.1.4 but without debug, io, os and (most of the) math modules
- Asynchronous event-driven programming model
- More than 65 built-in modules
- Firmware available with or without floating point support (integer-only uses less memory)

LFS allows Lua code and its associated constant data to be executed directly out of flash-memory; just as the firmware itself is executed. This now enables NodeMCU developers to create Lua applications with up to 256Kb Lua code and read-only constants executing out of flash. All of the RAM is available for read-write data.

NodeMCU is an open source IoT platform. It includes firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module. In this project, NodeMCU forms the brain of the smart door lock. The NodeMCU retrieves data from the cloud database and makes the relay ON/OFF according to the data.

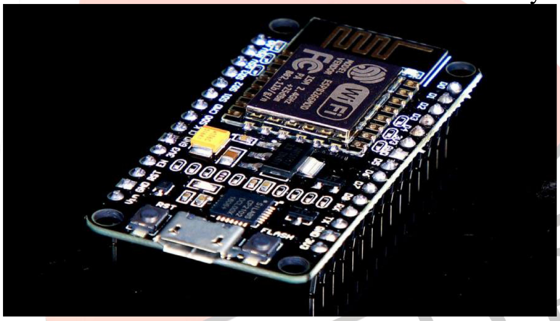


Fig. 4: ESP8266 Wifi Module

Electronic Door Lock

Electronic door locks are a way to replace keys or to add additional automation features, like remote locking or unlocking. Although most commonly found on cars, many cutting-edge security providers are offering electronic door locks for homes and businesses.

In any type of door lock, a latch or bolt is made to cross the opening between the side of the door and the doorframe, preventing access. This can be a “spring bolt,” which is held in place by springs and allows the door to close (but not reopen) when locked, or the more secure “dead bolt,” which stays in place until manually unlocked. In both cases, locking and unlocking is achieved by rotating the visible element (a knob or a key in a lock cylinder) to move the bolt or latch.

The electric door lock module operates at 12V which locks when the power is OFF and unlocks when the power is ON. It forms the physical part of the smart door lock.

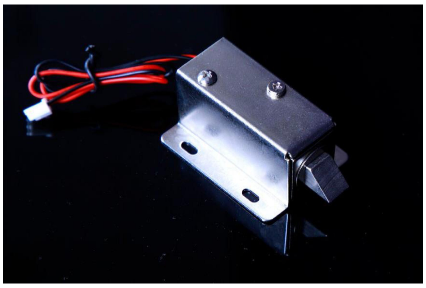


Fig. 5: Electronic Door Lock

5V Relay Module

Relays are most commonly used switching device in electronics. There are two important parameters of the relay. One is the Trigger Voltage and other is Load Voltage & Current. Our relay here has 5V trigger voltage. Since the relay has 5V trigger voltage we have used a +5V DC supply to one end of the coil and the other end to ground through a switch. This switch can be anything from a small transistor to a microcontroller or a microprocessor which can perform switching operation.

Features of 5-Pin 5V Relay:

- Trigger Voltage (Voltage across coil) : 5V DC
- Trigger Current (Nominal current) : 70mA
- Maximum AC load current: 10A at 250/125V AC
- Maximum DC load current: 10A at 30/28V DC
- Compact 5-pin configuration with plastic moulding
- Operating time: 10msec Release time: 5msec
- Maximum switching: 300 operating/minute (mechanically)

A relay is a switching device as it works to isolate or change the state of an electric circuit from one state to another. The 12V supply is given to the electric lock module using the Relay according to the data given by the NodeMCU.

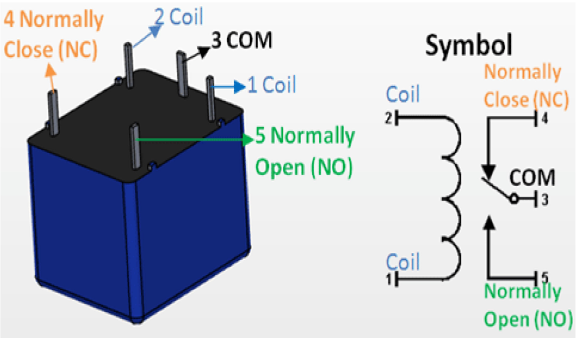


Fig. 6: 5-pin Relay Module

Sensors

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A Sensor converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically. We have used motion sensor, ldr, fire alarm, etc in this project.

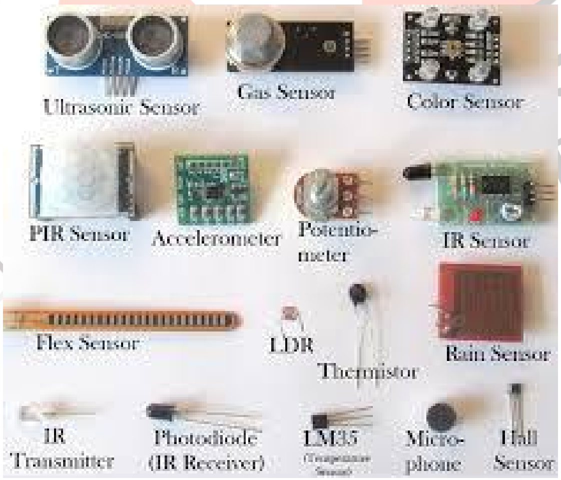


Fig. 7: Multiple Sensors

LDR

LDR is a component that has a (variable) resistance that changes with the light intensity that falls upon it. This allows them to be used in light sensing circuits.

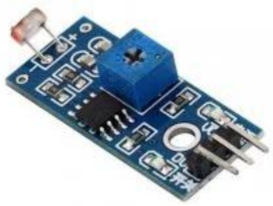


Fig. 8: LDR Sensor

Passive Infrared/Motion Sensor

Photosensors are also active motion sensors. They emit light (for example, a laser), and then if something blocks that light the sensor is triggered. Passive motion sensors pick up infrared signals put off by body heat. If the sensor notices an infrared energy, the motion detector is triggered and an alarm may sound.

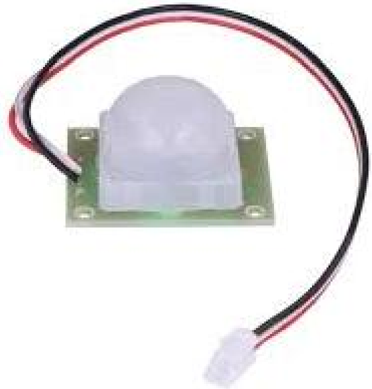


Fig. 9: PIR Motion Sensor

Fire Alarm

A fire detector works by detecting smoke and/or heat. Since a fire detector usually works by detecting smoke and/or heat, and not actual fire, these devices are not usually called "fire detectors". Instead, these devices are more appropriately called "smoke detectors" and "heat detectors".

Fig. 10: Fire Sensor

V. SOFTWARE

IFTTT- IFTTT helps you connect all of your different apps and devices. When you sign up for a free account, you can turn on Applets that help your apps and devices work together to do specific things they couldn't do otherwise.

Adafruit.io- Adafruit IO is a system that makes data useful. Our focus is on ease of use, and allowing simple data connections with little programming required. IO includes client libraries that wrap our REST and MQTT APIs. IO is built on Ruby on Rails, and Node.js.

The Mobile Application

Android studio

We need Android studio software here to build an application for finger print and face detection to unlock the door.

Our application includes user login and its credentials to detect and recognize the user identity. Our application program needs a smart phone with finger print sensor to use finger print detection.

Our application detect and recognize the user identity and send signals to NodeMCU to switch the relay on and to turn the door lock open.

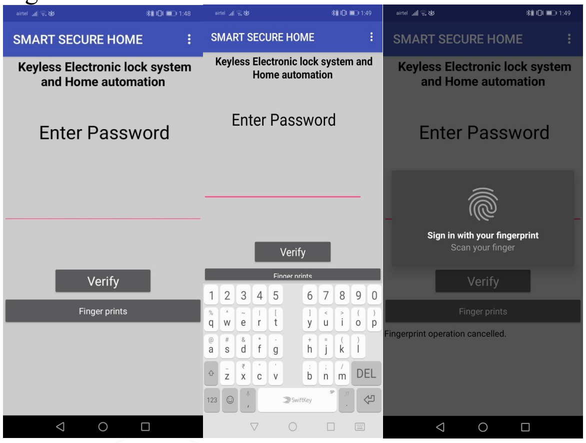
Features of Android Studio:

- Extensive testing tools and frameworks
- Lint tools to catch performance, usability, version compatibility, and other problems
- C++ and NDK support
- Built-in support for Google cloud platform, making it easy to integrate Google Cloud Messaging and App Engine.
- A mobile application is used to scan the fingerprint and to verify the fingerprint and authorize the person. Once the fingerprint is verified the key for unlocking is posted to firebase real-time database. The application is made using

Android Studio. The screenshots of the design and code blocks are attached. Design the application as shown and code block to give it life. If you are not interested in building the app just pay and download.

VI. RESULTS

Android Application Stepwise building:


SMART SECURE HOME
Keyless Electronic lock system and Home automation
Enter Password
Verify
Finger prints
SMART SECURE HOME
Keyless Electronic lock system and Home automation
Enter Password
Verify
Finger prints
SMART SECURE HOME
Keyless Electronic lock system and Home automation
Enter Password
Verify
Finger prints

Sign in with your fingerprint
Scan your finger

Fingerprint operation cancelled.

Fig. 11: User Login with e-mail ID, password given by owner and Fingerprint scanner

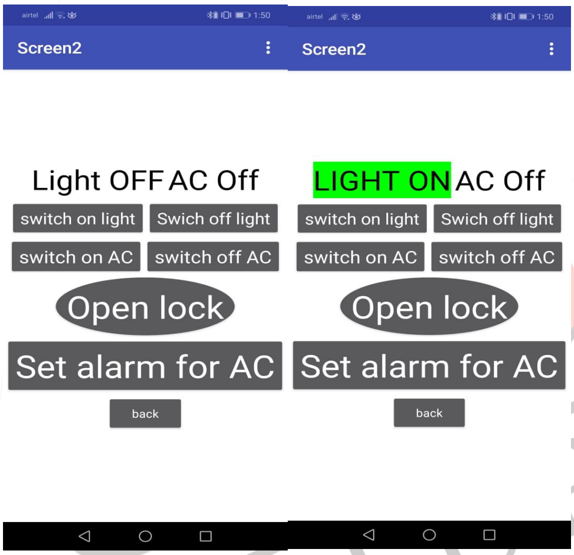


Fig. 12: Control Panel to control the AC Appliances from the Android Application

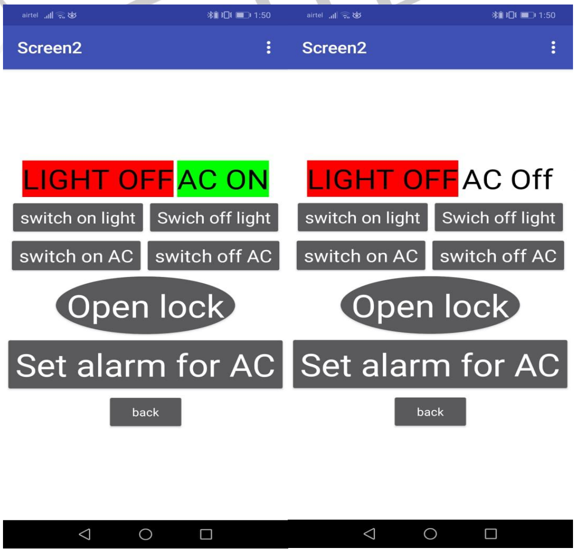
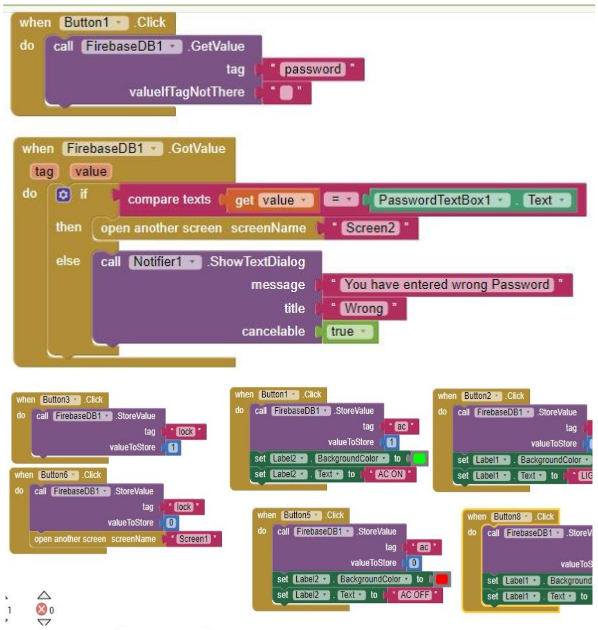
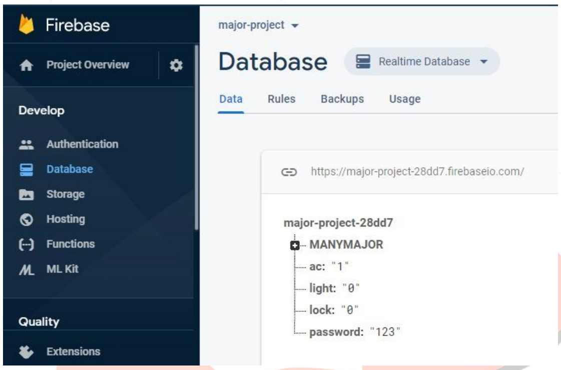


Fig. 13: Control Panel to control the AC Appliances from the Android Application with coloured buttons at ON and OFF State



```
when Button1 .Click
do  call FirebaseDB1 .GetValue
                        tag  " password "
          valueIfTagNotThere  "  "

when FirebaseDB1 .GotValue
  tag  value
do  if  compare texts  get value  =  PasswordTextBox1 . Text
    then  open another screen  screenName  " Screen2 "
    else  call Notifier1 .ShowTextDialog
                        message  " You have entered wrong Password "
                          title  " Wrong "
                     cancelable  true

when Button3 .Click
do  call FirebaseDB1 .StoreValue
                  tag  " lock "
         valueToStore  1

when Button6 .Click
do  call FirebaseDB1 .StoreValue
                  tag  " lock "
         valueToStore  0
    open another screen  screenName  " Screen1 "

when Button1 .Click
do  call FirebaseDB1 .StoreValue
                  tag  " ac "
         valueToStore  1
    set Label2 . BackgroundColor to 🟩
    set Label2 . Text to " AC ON "

when Button2 .Click
do  call FirebaseDB1 .StoreValue
                  tag
         valueToStore
    set Label1 . BackgroundColor
    set Label1 . Text to " LIG

when Button5 .Click
do  call FirebaseDB1 .StoreValue
                  tag  " ac "
         valueToStore  0
    set Label2 . BackgroundColor to 🟥
    set Label2 . Text to " AC OFF "

when Button8 .Click
do  call FirebaseDB1 .StoreV
         valueToS
    set Label1 . Background
    set Label1 . Text to
```

Fig. 14: Block Codes of the Android Application



```
https://major-project-28dd7.firebaseio.com/

major-project-28dd7
  MANYMAJOR
    ac: "1"
    light: "0"
    lock: "0"
    password: "123"
```

Fig. 15: Setting up the Google Firebase

VII. CONCLUSION

The implemented system is very cost effective. It is very easy to install and configure the system. The system provides different modes of operation (Single User, Multi User, Multi-Level), which makes the system more attractive and useful.

Simulation results and Experimental results vary, as simulation was done on the available library contents of software and considering ideal conditions. In the present system, the user can operate the home appliances within a range of 15 meters by pairing their android Bluetooth with Bluetooth module and the secure android app are used to open the door using fingerprint and given passwords. The overall system works on a very low voltage, within a range of 5V, providing electrical safety. The door lock as well as the home automation system is only powered ON when finger print matches with the enrolled fingerprints. In this automation project, the distance between control unit and android device is limited. On the basis of concept used in proposed system an industry oriented system can be developed. Biometric security systems can be implemented in key areas as banks, safe locks, etc. The system can be made more secure by adding the feature of sending SMS to the owner when any wrong finger print is scanned. We have used an amalgamation of various sensors so as to automate the lighting system. When someone enters the house, the motion sensor will detect it and switch on the lights in the areas when and where it is required. When the sun sets, the LDR will switch it on. Fire sensor will send in the notification to our phone in case there is fire anywhere in the house. This makes it convenient for the user so as to be relaxed with small things in life. Google assistant and the app works together with the hardware so as to provide ease of use to the user.

REFERENCES

[1]. M. Asadullah and A. Raza, "An overview of home automation systems," 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI), Rawalpindi, 2016, pp. 27-31, doi: 10.1109/ICRAI.2016.7791223.

[2]. M. Jerabandi and M. M. Kodabagi, "A review on home automation system," 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bangalore, 2017, pp. 1411-1415, doi: 10.1109/SmartTechCon.2017.8358597.

[3]. H. K. Singh, S. Verma, S. Pal and K. Pandey, "A step towards Home Automation using IOT," 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-5, doi: 10.1109/IC3.2019.8844945.

[4]. S. Soumya, M. Chavali, S. Gupta and N. Rao, "Internet of Things based home automation system," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2016, pp. 848-850, doi: 10.1109/RTEICT.2016.7807947.

[5]. A. Gurek, C. Gur, C. Gurakin, M. Akdeniz, S. K. Metin and I. Korkmaz, "An Android based home automation system," 2013 High Capacity Optical Networks and Emerging/Enabling Technologies, Magosa, 2013, pp. 121-125, doi: 10.1109/HONET.2013.6729769.

[6]. K. Mandula, R. Parupalli, C. A. S. Murty, E. Magesh and R. Lunagariya, "Mobile based home automation using Internet of Things(IoT)," 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, 2015, pp. 340-343, doi: 10.1109/ICCICCT.2015.7475301.

[7]. S. Dey, A. Roy and S. Das, "Home automation using Internet of Thing," 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, 2016, pp. 1-6, doi: 10.1109/UEMCON.2016.7777826.

[8]. H. K. Singh, S. Verma, S. Pal and K. Pandey, "A step towards Home Automation using IOT," 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-5, doi: 10.1109/IC3.2019.8844945.

[9]. A. Akhtar, T. Ahmad, N. Sabahat and S. Minhas, "IoT Based Home Automation System Using ThingSpeak," 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), London, United Kingdom, 2019, pp. 163-168, doi: 10.1109/iCCECE46942.2019.8941737.

[10]. S. Somani, P. Solunke, S. Oke, P. Medhi and P. P. Laturkar, "IoT Based Smart Security and Home Automation," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-4, doi: 10.1109/ICCUBEA.2018.8697610.

[11]. P. S. Nagendra Reddy, K. T. Kumar Reddy, P. A. Kumar Reddy, G. N. Kodanda Ramaiah and S. N. Kishor, "An IoT based home automation using android application," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 285-290, doi: 10.1109/SCOPES.2016.7955836.