Arduino Based Smart Fingerprint Authentication System

Meenakshi N
Ass.Prof at Dept. of .Information Technology
Hindustan Institute of Technology and Science
Chennai,India
nmeenakshi@hindustanuniv.ac.in

Monish M
Department of Information Technology
Hindustan Institute of Technology and Scinece
Chennai,India
monishmogi@gmail.com

Dikshit K J
Department of Information Technology
Hindustan Institute of Technology and Scinece
Chennai,India
dikshitdeepa0@gmail.com

Bharath S
Department of Information Technology
Hindustan Institute of Technology and Scinece
Chennai,India
bharathsukumaran97@gmail.com

Abstract

Security is the serious issue looked by everybody when we are far from our family unit. In the present situation acceptable answer for the above issue isn't yet found. Introduced here is an electronic securing framework which Arduino assumes the job of the preparing unit. Arduino which is a microcontroller board has a place with at uber family. It is an open source straight forward instrument. It can detect, screen, store and control application. Access control for the entryway is accomplished utilizing Arduino Mega 2560 board. This task displays a keyless framework for locking and opening purposes utilizing a predefined PICTURE secret key and OTP. Unauthorized person access is ensured by sending OTP and PICTURE password to ADMIN to get OTP and PICTURE password where the person needs to contact the ADMIN to get OTP and PICTURE password. It is entered through the 2.8" TFT touch display, which display all the UI messages and takes inputs from user. In case of authorized user, the system allows fingerprint sensor to validate the person followed by sending either PICTURE password or OTP via SIM using GSM module to the user registered mobile number saved in database (local SD card) in order to access the door. If the entered password matches, door will be opened automatically otherwise a message showing incorrect password will be displayed on TFT display and a notification will be sent to the owner that the security was tried to be breached. This hardware project achieves 3 levels of security with commonly available component and also consumes less power. This system also has an option to unlock the door through SMS in case of emergency by the ADMIN.

Keywords :- Fingerprint Lock system, OTP, Image password, three level security.

I. INTRODUCTION

Now a days Home, offices, shops, banks need high level security for safety purpose. To provide security for these field smart lock system is introduced. There are many innovative smart door locks are invented to lock and unlock the system. These type of has fingerprint, RFID card, pin, password or IOT by unlocking the system using mobile phone. These systems have same advantages and disadvantages and this type of security locks has any one security level to unlock the system from the provided security level. User using these types of locking system either uses pin number or fingerprint or RFID card to unlock the system. These system does not have security level chain to increase the security. To increase the security the user should unlock the system by minimum two security level. In home lock system there should be unlocking option for guest. Sometime thief may miss use the option and get into the home. So, we can provide two level of security for guest also. This process should be done with the use of admin for security purpose.

In our Fingerprint lock system there are three level of security where user can unlock the system by using any two level of security out of three levels. This produce high security where any unauthorized person tries to unlock, alert message is sent to the admin in first attempt itself. The system process fingerprint authentication, OTP which means one time password, Image password. The system is unique then other door locking system. Where the system process two level security out of three level security levels. In this system guest also has to cross two level security with the help of admin.

The Existing system in the market has fingerprint authentication, pin, IOT which is used to access the device using mobile phone or internet. In some devices the system in unlocked using generating OTP using GSM (global system for mobile) which is used to change the password instead of fixed password. Hacker or unknown person can unlock the system by various attack as brute force attack when the system as fixed password. In fingerprint security, unknown person can produce duplicate fingerprint impression in the fingerprint module. Pin or password based security lock can be attacked by brute force attack or watched live when user not noticing the surrounding. So there are some disadvantages in every system.

To increase the security level for locks, this lock system has implemented the three level security. Authorized

978-1-7281-1603-7/XX/$XX.00 ©2019 IEEE

user can unlock the system by first producing his fingerprint which is already registered with a particular registered ID, after fingerprint authentication the user who produced the fingerprint is sent an OTP message using GSM message. The mobile number of the user in registered with the user fingerprint. In other case user can unlock the system by image password. Here an image has fixed as password for particular user. Image password is registered to user fingerprint. If guest arrives, guest has to get into the guest option. In guest option the image password is randomly changes the password for security purpose. The random password in sent has message to the admin, guest has to select the correct password using communication with admin. If the image password is correct then an OTP is sent to the admin else it returns to the main page. The advantage of this system is high security level for both authorized and guest users. And fingerprint enrollment for new user and mobile number registering is done by admin using the system

II. EXISTING SYSTEM

The Existing system has few digital techniques for Door security locks. This modern smart locking systems replace the role of traditional locking system which has lock and keys. The drawback of these locks is they can be easily welded without any alert to the user. People want their home, office, shops to be secured. This need for people is the main reason for developing smart lock.

A. Fingerprint Locking System

Fingerprint locking system is a locking system using the user fingerprint with the help of fingerprint sensor module. The fingerprint sensor module the works with the help of Arduino or raspberry pi. The Fingerprint module checks the given fingerprint authorized or unauthorized. The locking system uses the user fingerprint to unlock the system [2].

B. Pin / Password Authentication

In Existing smart door lock Pin or password authentication is used along with the fingerprint authentication. It is used to unlock the system directly or used in the case of fingerprint failure. Most of the smart lock system pin number using keypad. The Existing systems has pin authentication to make users easy when fingerprint sensor is not working. And the main advice to the user is to not to share the pin number with the outsiders or typing pin number visible to unknown persons.

C. Internet of Things

IOT stands for internet of things which is worked in door lock through wireless connection. The user can access the door lock using his smart phone with the use of IOT supported apps. The user can easily unlock or lock the system by single touch. But IOT is supported only by internet connection.

D. RFID Card

The user can unlock the system by using RFID card stands for radio frequency identification. The radio frequency in scanned by the scanner and check whether the identity is authorized or unauthorized. The main drawback of this system is these cards can be duplicated by hackers. So the user has the handle it safely. The Existing systems in market had RFID card with other security types like fingerprint, pin authentication, IOT access, etc.

E. OTP Using GSM

OTP stands for one time password with is used for randomly changing the password for security purpose. OTP should be given in a particular time period otherwise the system will not recognize the password then the user has to refresh the OTP. The OTP is sent as a message using GSM modem which is used the send message to the registered mobile number.

Prof. Benazir H.M (2017) the author has discussed that, in the present current world, security assumes an essential job. For that reason, we proposed development security frameworks for managing an account locker framework and the bank clients. In this task we structure and actualize locker high security framework dependent on finger print, secret word and GSM innovation which can be composed in banks, ensured office and homes. It diminishes wastage of time for both broker just as client and gives propelled security. In this bank will gather the biometric information of every individual for allocating the lockers just credible individual can be recouped cash, records from the locker [7].

Akanksha singh (2015) the author has discussed, the way to control home machines, wellbeing and security framework utilizing GSM innovation by utilizing android application through android portable telephone. We will likewise demonstrate that we can control the machines even without an android telephone by sending an ordinary SMS. The benefit of utilizing GSM innovation is that we can control the home machines from remote places anyplace on the planet. This framework enables the proprietor to control the machines and to get a criticism status of the home machines by sending directions in type of SMS just as through an android application. For the home security framework we are utilizing an antitheft detailing framework which will report the proprietor by ringing a caution and by sending a SMS. Additionally for the wellbeing framework in the event that of flame or gas spillage it will report the proprietor by sending a SMS and furthermore by ringing an alert. In this manner by utilizing GSM innovation, it gives the remote access to the gadgets to be controlled [4].

Raqibull Hasan (2015) the author has discussed planning and execution of a microcontroller based home security framework with GSM innovation have been exhibited and examined. Two microcontrollers with other fringe gadgets which incorporate Light Emitting Diode (LED), Liquid Crystal Display (LCD), Buzzer and Global System for Mobile Communication (GSM) Module are in charge of solid task of the proposed security framework. Furthermore, a cell phone is interfaced with microcontroller through a Bluetooth gadget so as to control the framework. Additionally, manual keypad is another approach to bolt or open the framework. A Compiler Code Vision AVR is utilized to plan a program that controls the framework alongside keeping up all security capacities. The planned program is connected in Proteus Software for recreation. Finally, the aftereffects of down to earth circuit demonstrate the best possible capacities and furthermore confirm the dependable security inside sensible expense [5].

F. *Limitation of Existing System*

- The Existing system some time fails to provide security by various attack by hacker or unknown persons.
- The Existing system has fingerprint authentication for door lock system which may be open by unknown person by duplicating the fingerprint impression of the user.
- Another way of opening the lock is pin or password authentication. Here the user has to keep his password secured. In some cases, the hackers may get the password using various attacks or by using the scanner to check the finger impression on the keys
- The main drawback of IOT device is, they can't work without internet, so in the case of failure of power supply IOT may not work. And if the IOT server is overloaded or error in server may became a problem
- Using RFID card to locking system is developed to make the user to easily lock or unlock the system. It is used in failure of pin and fingerprint, but these types of card can be duplicated.
- The drawback of the Existing system is, some system has more than one security in the same system but it requires any one authentication to unlock system
- Some system has two level authentication, but it can be easily hacked by hacker and guest can't be entered until the authorized user has to come and open the door.
- The process of changing the password and fingerprint is a difficult process in the Existing system.

III. PROPOSED SYSTEM

Our Proposed system overcomes all the security problems in the existing system and provides high security and efficiency. This is a perfect and optimal solution for saving one from the hassle of stolen/lost key or an unauthorized entry. The main advantage of our locking system is three level security where user has to face any two level of security to unlock the system. This process overcome the problems faced by the Existing systems. The Proposed system is used to provide high security to home, office, shops, etc. because as mentioned in above the Existing system can be hacked by cracking any one password which is produced in the system. So the Proposed system is mainly used for overcome the security issues.

A. *Components used for Proposed System*

We have built the system proposed system using five major components. Each component has some specific uses and different working process. Short definition about these components are given below.

- *Arduino Mega 2560*

Arduino Mega 2560 is a microcontroller board dependent on the ATmega2560. It has 54 advanced info/yield pins (of which 14 can be utilized as PWM yields), 16 simple sources of info, 4 UARTs (equipment sequential ports), a 16 MHz precious stone oscillator, a USB association, a power jack, an ICSP header, and a reset catch. It contains everything expected to help the microcontroller; just associate it to a PC with a USB link or power it with an AC-to-DC connector or battery to begin. The Arduino Mega can be controlled by means of the USB association or with an outer power supply. The power supply for the board ought to be 6 to 20 volts. Arduino Mega can be customized utilizing Arduino programming.

- *2.8" TFT Sheild*

This 2.8" TFT touchscreen is intended to appropriate for Arduino Mega 2560/UNO. It can straightforwardly connect to the Arduino Mega 2560 board with no wiring or welding. Library is perfect with Adafruit TFT touchscreen shield, which is anything but difficult to utilize. It has much more goals than a highly contrasting 128×64 showcase. As a reward, this showcase has a resistive touchscreen appended to it as of now, so you can distinguish finger presses anyplace on the screen. 240×320 pixels with individual pixel control. In the interim, this module underpins smaller than normal SD card to grow capacity.

- *R301 Fingerprint Sensor*

Unique finger impression sensor is utilized for client ID. This is utilized for record distinguishing proof which give security to singular records. Unique mark handling incorporates two sections: finger impression enlistment and unique finger impression coordinating. While selecting client needs to enter the finger multiple times. The framework will process the two time finger picture, create a format of the finger dependent on handling results and store the layout. While coordinating, client enters the finger through optical sensor and framework will produce a format of the finger and contrast it and layouts of the finger. Framework will contrast the live finger and explicit layout assigned in the module. In the event that the live unique mark is coordinated the framework continue effectively, else it is disappointment.

- *Buzzer*

Typically signal is utilized for giving ready when any unapproved passage is done or acknowledge is occurred. There are two sorts of ringer to be specific dynamic and inactive signal. A functioning bell will create a tone utilizing an inner oscillator, so all that is required is a DC voltage. An aloof ringer requires an AC flag to make a sound. In this framework, signal works when any illicit sections is done or when any unapproved people attempts to open the framework.

- *SIM900A GSM Module*

In this framework we utilizes SIM900A GSM module for sending OTP message to enlisted client. GSM module is utilized to build up correspondence between a PC and a GSM framework. GSM is a design utilized for portable correspondence is the majority of the nations. GSM module comprises of GSM modem gathered together with power supply circuit and correspondence interface for PC. GSM modem can play out the accompanying tasks like Receive, send or erase SMS messages in a SIM or Read, include, look phonebook sections of the SIM or Make, get or dismiss a voice call.

B. *Software and Programming*

The following software is used to build the proposed system:

- *Arduino software.*
- *Language used in 'c' program.*

The system uses Arduino mega 2560 as the microcontroller which is used to connect the other parts and process the working of these parts. So we use Arduino software to give instruction in a form of program (c language) to the board.

IV. BLOCK DIAGRAM

The block diagram (Fig.1) explains the connection of the proposed system. Arduino mega 2560 act as the microcontroller which plays main roll in the system. Fingerprint sensor, keypad in TFT display and image password are the input given to unlock the system. The output will be unlocking the system. The power supply to the Arduino board is by USB or by additional power supply. SD card is connected to the Arduino to store the data like images and fingerprints is stored as fingerprint image or fingerprint template in the fingerprint sensor module. The TFT display shows the instruction for the input and display the input is correct or wrong. If the inputs given is correct it displays correct, else wrong. Solenoid lock is used to open and close the system, if the input is correct the locked system is unlocked by instruction given by Arduino. Else it returns to the first page.

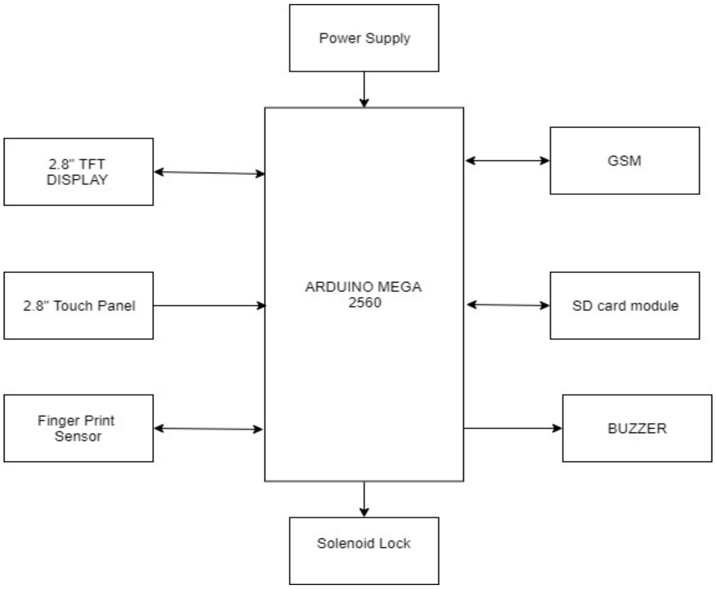

Fig.1. *Block Diagram*

V. WORKING

The flowchart (fig 2) given below clearly explains the working of "fingerprint lock system". The working process is started by differentiate the user into authorized and unauthorized user. Both user has to face any two level security out of three. But unauthorized user can unlock the system by communicating with admin to tighten the security. If unauthorized person tries to unlock the system without the admin knowledge, alert message is sent to admin and sound alert is turned on by buzzer. Let's see the process carried by authorized and unauthorized persons.

A. *Authorized person*

- The authorized person as to enroll his fingerprint in the system. Then the mobile number of the registered person is included in GSM and a permanent image password is fixed to this user.
- As the first step, the user has to choose the type of user. He/she has to select authorized user.
- Then they have to give their fingerprint to the fingerprint sensor. After entering fingerprint, system checks whether the input fingerprint is registered or not.
- If the given fingerprint is authorized, then the system send an OTP to the mobile number of the fingerprint ID. Else the given fingerprint is unauthorized the system returns to the first page.
- Or the system shows set of image where user has to select the image password fixed to him.
- The OTP and image password is randomly select by the system. If the OTP or Password is incorrect then the system returns to the first page.

- After giving correct OTP or image password the system in unlocked.
- If the input given went wrong for three times then system locks for a particular time and buzzer starts alert.

B. *Unauthorized person*

- The unauthorized person has to select user type as unauthorized as the first step. A random image is sent to the admin. Person has to select the random image correctly. Else the system returns to the first page.
- The image password is changed to next attempt which is also sent to admin. System verify the select image is correct or not. If the selected image is correct then OTP is sent to the admin.
- Person has to enter the OTP correctly to unlock the system. Else, the system returns to the first page.
- Unauthorized person can do these actions only by communicating with admin for security purpose. This option is used for guest visit or urgent entries or help purpose.

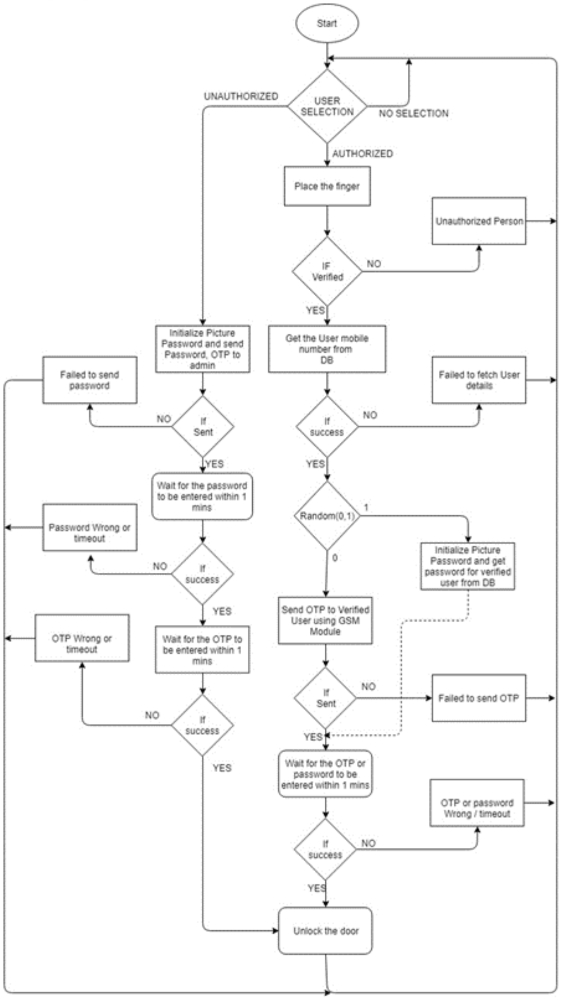
Start
UNAUTHORIZED
USER SELECTION
NO SELECTION
AUTHORIZED
Place the finger
Unauthorized Person
IF Verified
NO
YES
Initialize Picture Password and send Password, OTP to admin
Get the User mobile number from DB
Failed to send password
Failed to fetch User details
NO
If Sent
If success
NO
YES
YES
Wait for the password to be entered within 1 mins
Random(0,1)
1
Password Wrong or timeout
Initialize Picture Password and get password for verified user from DB
NO
If success
0
YES
Send OTP to Verified User using GSM Module
OTP Wrong or timeout
Wait for the OTP to be entered within 1 mins
NO
If Sent
Failed to send OTP
NO
If success
YES
YES
Wait for the OTP or password to be entered within 1 mins
OTP or password Wrong / timeout
If success
NO
YES
Unlock the door

Fig 2. *Proposed System Flowchart*

C. *Related System VS Proposed System*

We have already seen the existing system and what are all the methods carried out by existing system. Now existing system is compared with proposed system and usage of proposed system instead of existing system is discussed

- The Proposed system has three level of security but existing system has maximum two levels of security.
- The user can unlock the system by any two ways, in Existing system has only two options. It can lead to low security for doors.
- The Proposed system has option to guest to unlock the system, Existing system has no option like that. Guest has to wait for the user to unlock the system.
- Security level is accurate than Existing system.
- In some related system, users use the IOT technology to unlock the system for guest. It may some time goes wrong.
- In the Proposed system has some terms to unlock the system with admin knowledge.
- Proposed system alternatively has image password instead of OTP with system randomly ask any one authentication.
- In guest option the image password changes to every attempt. Admin receives the changes password which is sent as a message.
- Some of the Existing system allows user to unlock the system by any one options. It may lead to security issue.

D. *Advantages of Proposed System*

- Image password as a third security level
- Highly accuracy in term of security
- Relatively low cost so that everyone can use at their home, offices, shops, etc.
- Fingerprint enrollment is easier.
- Unlocking the system using any two security levels out of three security levels
- It helps to keep the place secure then other devices
- Alert message is sent when the first level is wrong, hence the user is alerted soon.
- No false intrusion
- No manual errors
- Maintenance of time

E. *Disadvantaged of Proposed System*

- Admin has to be alert on the notification from the system
- Users has to keeps their mobile phone secured, because hacker can hack their phone to get OTP and hacker may block the notification if they hack the phone

F. Application of Proposed System

- Security for homes
- Security for shops
- Secured offices, industries, server room
- Secures locker, gun box, bank lockers, etc.

CONCLUSION & FUTURE STUDY

In present situation, there are possibilities to hack and unlock the smart locks. The proposed system can overcome the security issues faced in the present situation. The 3 level security in the system can help the user for accurate security. The main reason for the proposed system is to secure the user living place, working place or to keep their valuable things, documents in a protected way. Hence this project can be understood by peoples and future work can be done. Various technology and update can be performed is the project. This project can be rebuilt by various microcontroller and various methods.

ACKNOWLEDGMENT

We would like to express our special thanks of gratitude to our project guide Ms.N.Meenakshi Madam as well as to our coordinator B.Dwarakanath sir who gave us the golden opportunity to do this wonderful project on this topic (Arduino Based Smart Fingerprint Authentication System), which also helped us in doing a lot of research and we came to know about so many new things.

REFERENCES

[1] A.Aditya Shankar, P.R.K.Sastry, A.L.Vishnu ram, A.Vamsidhar, International Journal of Engineering and Computer Science (IJECS) “Finger Print Based Door Locking System” vol.4, issue03, december2015 (Reference).

[2] Manish Aggarwal, Department of Electronics and Communication Engineering , Elins International Journal of Science Engineering and Management ”Secure Electronic Lock Based on Bluetooth Based OTP System” vol.2, Issue1, January 2017.

[3] Pavithra.B.C, Myna.B.C, kavyashree.M Fingerprint Based Bank Locker System Using Microcontroller Proceeding of IRF International Conference, 5 April -2014, Pondicherry, India, ISBN: 978-93-82702-71-9.

[4] Akanksha singh, arijit pal, bijay rai, “GSM Based Home Automation, Safety and Security Using Android Mobile Phone”, International Journal of Engineering Research & Technology(IJERT), vol.4, Issue 5, May 2015.

[5] Raqibull Hasan, Mohammad Monirujjaman Khan, Asaduzzaman Ashek, Isarat Jahan Rumpa, “Microcontroller Based Home Security System with GSM Technology” open Journal of Safety Science and Technology, 2015,5,55-62 Published online June 2015 in sciRes

[6] Vini Madan, S.R.N Reddy, “GSM-Bluetooth based remote monitoring and control system with automatic light controller “, International Journal of Computer Applications, vol 46-No.1,may 2012.

[7] Prof.Benazir.H.M Dept. of ECE, Nisha S. Kalpathri, Chandralekha Sunagar, Shaikh Collage of Engineering and Technology, Belagavi, India “Fingerprint Authentication Smart Locking System Using OTP”, International Journal of Advance Research in Engineering, Science & Technology, vol 4, Issue 6, June-2017.

[8] Mr.Patil Bhushan S, Mr.Mahajan Vishal A, Mr.Suryawanshi Sagar A, Mr.Pawar Mayur B, Prof.Mr.U.R.Patole, “ Automatic Door Lock System using PIN on Android Phone”, International Research Journal of Engineering and Technology, vol 05, Issue 11, November 2018.

[9] Sri Prakash N, Venkatram N. “Establishing efficient Security scheme in home IOT device through biometric finger print technique”. Indian Journal of Science and Technology, 2016 May.

[10] Jason Johnson and Christopher Dow, “Intelligent door lock system with encryption”, US patent Application Publication Johnson et al., pp. 1-92, June 2016.

[11] Mustafijur Rahman, A. H. M. Zadildul Karim, Sultanur Nyeem, Faisal Khan, and Golam Matin; "Microcontroller Based Home Security and Load Controlling Using GSM Technology"; I. J. Computer Network and Information Security, 2015.

[12] Rohit Kadam, Pranav Mahmauni, and Yash Parikh; "Smart Home System"; International Journal of Innovative research in Advanced Engineering (IJIRAE), Vol. 2, Issue 1, 2015.

[13] Nazrul□ Anuar□ Nayan, Ili A. M. Ikhsan, and Yasuhiro Takahashi; "Using ZigBee Communication Technology in a Smart Home Wireless Sensor Network"; Proceedings of Second International Conference on Modern Trends in Science, Engineering and Technology, 2014.

[14] Rajeev Piyare and Seong Ro Lee; "Smart Home Control and Monitoring System Using Smart Phone"; ICCA 2013, ASTL Vol. 24, pp. 83 - 86, 2013.

[15] Jayashri B. Angali and Arvind Shaligram; "Design and Implementation of Security Systems for Smart Home based on GSM Technology"; International Journal of Smart Home, Vol. 7, No. 6, pp. 201-208, 2013.