

THREE TIER HOME SECURITY USING GSM TECHNOLOGY

A PROJECT REPORT

Submitted by

AKSHAI K.P (311613104005)

DHARANENDIRAN.C (311613104020)

MANOJ S.H (311613104053)

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING



MISRIMAL NAVAJEE MUNOTH JAIN ENGINEERING COLLEGE

CHENNAI

ANNA UNIVERSITY::CHENNAI 600 025

APRIL 2017

ANNA UNIVERSITY :: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report “**THREE TIER SECURITY USING GSM TECHNOLOGY**” is the bonafide work of “**AKSHAI K.P (311613104005), DHARANENDIRAN.C (311613104020), MANOJ.S.H (311613104053)**” who carried out the project work under my supervision.

SIGNATURE

Mrs.P.Asha M.E., (Ph.D)

HEAD OF THE DEPARTMENT,

Department of CSE,

Misrimal Navajee Munoth Jain

Engineering College,

Thoraipakkam, Chennai-97.

SIGNATURE

Mrs.B.Yasotha B.E., M.Tech., (Ph.D)

SUPERVISOR,

ASSISTANT PROFESSOR

Department of CSE,

Misirimal Navajee Munoth Jain

Engineering College,

Thoraipakkam, Chennai-97.

Submitted for the Anna University VIVA-VOCE Examination held on _____.

INTERNAL EXAMIER

EXTERNAL EXAMIER

ACKNOWLEDGEMENT

We express our gratitude and sincere thanks to our honorable secretaries **Dr. Harish L Mehta (SecretaryAdministration)** and **Shri L. JaswantMunoth (SecretaryAcademic)** for providing the infrastructure facilities to do this project during our course period.

We thank our **Principal, Dr.C.Chandrasekar Christopher, M.Tech., Ph.D.**, for his support and motivation for the development and completion of this project.

We express profound sense of gratitude and heartfelt thanks to our **Head of the Department, Mrs.P.Asha, M.E (Ph.D.), ASSOCIATE PROFESSOR**, Department of Computer Science and Engineering for her kind words and enthusiastic motivation which inspired us a lot in completing this project.

We would like to express our gratitude to our project guide **Mrs. B.Yasotha B.E, M.Tech., (Ph.D), ASSISTANT PROFESSOR**, Department of Computer Science and Engineering and to our Project Coordinator **Ms.B.Padmaja M.E., ASSISTANT PROFESSOR**, Department of Computer Science for their valuable suggestions and constant encouragement that led to the successful completion of the project.

Finally, we thank all the Teaching and Non-Teaching Staff members of our Department who helped us to complete this project. Above all we thank the Almighty, Our Parents and Siblings for their constant support and encouragement for completing this project.

ABSTRACT

Security and automation is a prime concern in our day-to-day life. Home security system is needed for convenience and safety. This system invented to keep home safe from intruders and hazardous situations. We have proposed the design and implementation of a microcontroller based home security system with GSM technology. The designed program is applied in Arduino for simulation. Security has becoming an important issue everywhere. Home security is becoming necessary nowadays as the possibilities of intrusion are increasing day by day. Safety from theft, leaking of raw gas and fire are the most important requirements of home security system for people. A traditional home security system gives the signals in terms of alarm .However, the GSM (Global System for Mobile communications) based security systems provides enhanced security as whenever a signal from sensor occurs, a text message is sent to a desired number to take necessary actions. Although advanced biometric authentication methods such as fingerprints and iris identification can further identify the user who is requesting authorization, they incur high system costs and access privileges cannot be transferred among trusted users. We have tried to increase these standards by combining new design techniques and developed a low cost home and industrial automated security system.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	iv
	LIST OF FIGURES	vii
	LIST OF ABBREVIATIONS	viii
	LIST OF SYMBOLS	xi
1	INTRODUCTION	1
	1.1 GENERAL	1
	1.2 AUTHENTICATION METHODS	1
2	LITERATURE SURVEY	3
3	SYSTEM ANALYSIS	8
	3.1 EXISTING SYSTEM	8
	3.1.1 Drawbacks	8
	3.2 PROPOSED SYSTEM	9
	3.1.2 Advantages	9
4	HARDWARE / SOFTWARE DESCRIPTION	10
	4.1 HARDWARE DESCRIPTION	10
	4.1.1 Power Supply	10
	4.1.2 Microcontroller – Arduino UNO R3	14
	4.1.3 RFID – RC522	14
	4.1.4 Bluetooth – HC05 – 06	15
	4.1.5 Servo Motors	15
	4.1.6 Odor Sensor – MQ2/MQ3	15
	4.1.7 GSM Module	15

	4.2 SOFTWARE DESCRIPTION	16
	4.2.1 C Language	16
5	SYSTEM DESIGN	17
	5.1 STRUCTURE OF THE SYSTEM	17
	5.2 SYSTEM ARCHITECTURE	18
	5.3 MODULES	20
	5.3.1 RFID Servomotors	
	Implementation	20
	5.3.2 Precautions in case	
	Of Breach Access	23
	5.3.3 Odor Sensor	
	Implementation	24
	5.4 DATA FLOW DIAGRAM	24
	5.5 UML DIAGRAM	26
	5.5.1 Use Case Diagram	26
	5.5.2 Activity Diagram	27
	5.5.3 Sequence Diagram	28
	5.5.4 Collaboration Diagram	29
6	CONCLUSION	31
	APPENDICES	32
	APPENDIX – 1 SAMPLE CODE	32
	APPENDIX – 2 SCREENSHOTS	42
	REFERENCES	48

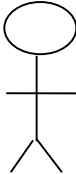
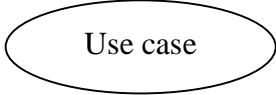
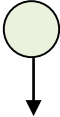

LIST OF FIGURES


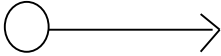
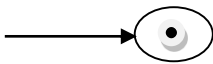
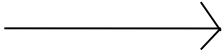
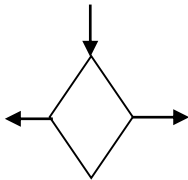
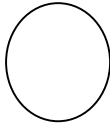
FIGURE NO.	TITLE	PAGE NO.
4.1.1	BLOCK DIAGRAM (Power Supply)	10
4.1.1.1	+5/+12V CIRCUIT DIAGRAM	11
5.2.1	SYSTEM ARCHITECTURE	19
5.2.2	PIN DIAGRAM	20
5.3.1	AUTHENTICATION AND DOOR LOCK	21
5.3.1.1	WORKING OF REED SWITCH	21
5.3.1.2	SERVO DIAGRAM	22
5.3.1.3	BLUETOOTH MODEL WORKING	22
5.3.2	IR-SENSOR-ILLUSTRATION	23
5.3.3	MQ2 AND MQ3 DIAGRAM	24
5.4.1	LEVEL 0 DATA FLOW DIAGRAM	25
5.4.2	LEVEL 1 DATA FLOW DIAGRAM	25
5.4.3	LEVEL 2 DATA FLOW DIAGRAM	26
5.5.1	USECASE DIAGRAM	27
5.5.2	ACTIVITY DIAGRAM	28
5.5.3	SEQUENCE DIAGRAM	29
5.5.4	COLLABORATION DIAGRAM	30

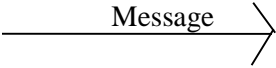

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
RFID	R ADIO- F REQUENCY I DENTIFICATION
GSM	G LOBAL S YSTEM FOR M OBILE
SMS	S HORT M ESSAGING S ERVICE
API	A PPPLICATION P ROGRAMMING I NTERFACE
GUI	G RAPHICAL U SER I NTERFACE
UML	U NIFIED M ODELLING L ANGUAGE
IR	I NFRA- R ED

LIST OF SYMBOLS

S.NO	NOTATION NAME	NOTATION	DESCRIPTION
1.	Actor		It aggregates several classes into single classes.
2.	Use case		Interaction between the system and external environment
3.	Initial State		Initial state of the object
4.	Communication		Communication between various use cases.

5.	State		State of the process.
6.	Initial State		Initial state of the object
7.	Final state		Final state of the object
8.	Control flow		Represents various control flow between the states.
9.	Decision box		Represents decision making process from a constraint
10.	Data Process /State		A circle in DFD represents a state or process which has been triggered due to some event or action.

11.	Message		Represents the message exchanged
12.	Transition		Represents Communication that occurs between states.

CHAPTER 1

INTRODUCTION

1.1 GENERAL

Home security has changed a lot from the last century and will be changing in coming years. Security is an important aspect or feature in the smart home applications. The new and emerging concept of smart homes offers a comfortable, convenient, and safe environment for occupants. Conventional security systems keep homeowners, and their property, safe from intruders by giving the indication in terms of alarm. However, a smart home security system offers many more benefits. Several modules like GSM, magnetic door sensors, RFID module, odor sensor, IR sensor, Bluetooth etc. The goal of this project is to utilize the after-market parts and build an integrated home security system. Consequently, the proposed system provides reliable security within reasonable cost and also removes the circuit complexity.

1.2 AUTHENTICATION METHODS

In this proposed model, we propose three-tier layer of security measures for any home or office situations. We consider three tiers, the tier 1 security concentrates in authenticating the genuine user to enter his/her house. The authentication is done using RFID tag where it is connected to an Servo motor for locking purpose and family members are given each a unique RFID card where there is an 16-bit key code each distinct from one other and still suffers from problems such as access RFID card losses. There is one master card for the main family person and remaining are all RFID tags, which are portable and used along with vehicle

keychain. In case, of a guest user or loss of RFID tag we implemented a new tier, which authenticates genuine users.

In Tier 2, we developed an Android App (Three Tier Security) where guests can register their data in our database and the owner receives this information and grants permissions to their guests in case the owner is out of town or our relatives need to stay in our house while owner is away. This is done by Bluetooth module and where guest pair with the Bluetooth module and access the door unlock button he/she gains access to the house. Same goes for owner losing his/her RFID tag or master card can access his/her home by Android App for Admin (TTS Admin) this is used only by Owner and it connects with Bluetooth module of Arduino and authenticates access.

In Tier 3, this is worst-case scenario detection of intruders via odor sensor, this is experimental and has been implemented as way to find gas leakage or fire accidents in the house. Also used to find owner using unique smell stored on the module.

CHAPTER 2

LITERATURE SURVEY

[1]Abhishek S. Parab (2015), ‘Implementation of Home Security System using GSM module and Microcontroller’

This system invented to keep home safe from intruder. In this work, we present the design and implementation of a GSM based wireless home security system. which take a very less power. The system is a wireless home network which contains a GSM modem and magnet with relay which are door security nodes. The system can response rapidly as intruder detect and GSM module will do alert home owner. This security system for alerting a house owner wherever he will. In this system a relay and magnet installed at entry point to a precedence produce a signal through a public telecom network and sends a message or redirect a call that that tells about your home update or predefined message which is embedded in microcontroller. Suspected activities are conveyed to remote user through SMS or Call using GSM technology. This system tested on the latest technology available in smartphone which gives a proper result. This system is easy to use and very simple. The model can be installed with a economical cost. The GSM technology gives a good response after received a message of particular action from microcontroller. SMS received time to house owner is basically depend on the signal strength range that you have got through mobile tower. We have developed and tested the model using C language further the same model can be enhanced with the help of some high end language and which would be more portable. This system tested on the latest technology available in smartphone which gives a proper result. This system is easy to use and very simple. The model can be installed with a economical cost. The GSM technology gives a good response after received a message of particular action from

microcontroller. SMS received time to house owner is basically depend on the signal strength range that you have got through mobile tower. We have developed and tested the model using C language further the same model can be enhanced with the help of some high end language and which would be more portable.

[2]Anandan R, Karthik B, Kiran Kumar Dr.T.V.U (2015), ‘Wireless Home And Industrial Automation Security System Using Gsm’

This wireless home and industrial automation and security system can be used to provide security system for residential, industrial, and for all domestic and commercial purposes using GSM technique. Security systems are certain electronic devices, which are used to detect intrusions in home or industry. The basic components of a home automation security system are motion detectors, LPG detectors and smoke detector. When the internal mode is selected by the user when they are inside the wireless security area, the entire sensor except PIR sensor will be activated and the buzzer connected with the microcontroller will give an alarm and the reason for the insecurity will be displayed in the LCD connected to the microcontroller. In this mode, the electrical appliances in the security area automatically change to the manual mode in which user will control it. When the external mode is selected by the user when they are outside the wireless security area, all the sensor will be active and the security area address which is pre-programmed, along with the problem will be sent as SMS to the specified police station, fire station, security room and also to the user at the time of insecurity, fire accident, unwanted movement of persons etc, which is sensed by the respective sensor.

[3]Chintaiah N, Rajasekhar K, Dhanraj V (2011), ‘Automated Advanced Industrial and Home Security Using GSM and FPGA’

Home and industrial security today needs to make use of the latest technological components. In this paper I going to present the design and implementation of a remote and sensing, control and home security system based on GSM (Global System for Mobile). This system offers a complete, low cost, powerful and user friendly way of 24 hours of real –time monitoring and remote control of a home and industrial security. The system works as a remote sensing for the electrical appliances at home to check whether it is on or off, at the same time the user can control the electrical appliances at home by sending SMS (Short Messaging Service) message to the system, for example turning on t he AC before returning home. In case of fire/security the chip will receive signals from the different sensors in the monitoring place and acts according to the received signal by sending an SMS message to user’s Mobile Phone, it also works as automatic and immediate reporting to the user in case of emergency for home security, as well as immediate and automatic reporting to the fire brigade and police station according to activated sensor to decrease the time required for tacking action. In this paper we introduced a remote sensing and control system based on using Global System for Mobil (GSM) and FPGA. The system is suitable for a real time monitoring in home security as well as controlling and sensing in home automation with large number of controlled devices. The system has been design and implemented in hardware using VHDL language and Xilinx Spartan 3E FPGA. GSM has been used for testing the circuit either for the sensing part of the circuit or the control part. The design was simulated and verified the correctness and working operation of the whole system

[4]Jayashri Bangali and Arvind Shaligram (2013), ‘Design and Implementation of Security Systems for Smart Home based on GSM technology’

Smart Home can be also known as Automated Home or intelligent home, which indicates the automation of daily tasks with electrical appliances used in homes. This could be the control of lights, fans, viewing of the house interiors for surveillance purposes or giving the alarm alteration or indication in case of gas leakage. Home security has changed a lot from the last century and will be changing in coming years. Security is an important aspect or feature in the smart home applications. The new and emerging concept of smart homes offers a comfortable, convenient, and safe environment for occupants. Conventional security systems keep homeowners, and their property, safe from intruders by giving the indication in terms of alarm. However, a smart home security system offers many more benefits. This paper mainly focuses on the security of a home when the user is away from the place. Two systems are proposed, one is based on GSM technology and other uses web camera to detect the intruder. The first security system uses a web camera, installed in house premises, which is operated by software installed on the PC and it uses Internet for communication. The camera detects motion of any intruder in front of the camera dimensions or camera range. The software communicates to the intended user via Internet network and at the same time, it gives sound alert. The second security system is SMS based and uses GSM technology to send the SMS to the owner. The proposed system is aimed at the security of Home against Intruders and Fire. In any of the above cases happens while the owners are out of their home then the device sends SMS to the emergency number which is provided to the system. The system is made up of three components: sensors, GSM-GPS Module (sim548c), Atmega644p microcontroller, relays to control the device and buzzers to give security alert signal in terms of sound.

[5]Raqibull Hasan, Mohammad Monirujjaman Khan, Asaduzzaman Ashek, Israt Jahan Rumpa (2015), ‘Microcontroller Based Home Security System with GSM Technology’

In this paper, design and implement of a microcontroller based home security system with GSM technology have been presented and analyzed. Two microcontrollers with other peripheral devices which include Light Emitting Diode (LED), Liquid Crystal Display (LCD), Buzzer and Global System for Mobile Communication (GSM) Module are responsible for reliable operation of the proposed security system. In addition, a mobile phone is interfaced with microcontroller through a Bluetooth device in order to control the system. Moreover, a manual keypad is another way to lock or unlock the system. At last, the results of practical circuit show the proper functions and also verify the reliable security within reasonable cost. This paper presents design and implementation of a smart home security system based on microcontroller along with GSM for user friendly application. The system is intelligent enough to monitor the secure environment. In addition, the user is informed about the security breach through GSM network that provides a special opportunity whenever the user stays at far away from home. However, Android application is the most stunning feature in order to control the system through a Bluetooth device. Moreover, the system provides the reliable operation within reasonable cost and removes the system complexity. In this work, traditional burglar alarm mode, LED lights and LCD are the promising features used to ensure reliability. The whole system is implemented on a practical home security system which requires considerable effort to install it. Consequently, the system is also applicable for commercial purposes due to versatile ways of security and controllability.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

- Most of the existing systems are not user friendly and are expensive too.
- False alarms are an extremely common problem of home security cameras. It is annoying to constantly receive alarms just because trees move in the wind or birds fly past your window.
- These security system needs proper installation and maintenance is necessary to keep the system functioning properly. (it should be done with their respective service engineers).
- Although advanced biometric authentication methods such as fingerprint and iris identification can further identify the user who is requesting authorization, they incur high system costs and access privileges cannot be transferred among trusted users.

3.1.1 Disadvantages

- Microcontroller malfunction due to overload modules.
- High system cost and access privileges cannot be transferred among trusted users.
- Older GSM modules have low signal precision and strength, which is not reliable.

3.2 PROPOSED SYSTEM

- It consists of three tiers (MAGNETIC DOOR/WINDOW SENSOR, MOTION TRACKING, and Odour SENSOR). This enhance the security and also accuracy rate. The alarm will be triggered only on the basis of appropriate constraints in its context.
- Since it consists of magnetic sensors, accuracy is improved, whereas traditional IR sensors may trigger false alarms based on naive intrusions.
- The proposed system can be easily accessible via mobile application (with/without INTERNET), with the live streaming of Motion Tracking Camera facilities.
- The proposed system is also power efficient.

3.2.1 Advantages

- Secure Registration and Recovery.
- Backward-compatible with existing modules and newer modules.
- Authentication accuracy of 90%.
- Cost effective and Energy less consumption than other market home based security systems.

CHAPTER 4

HARDWARE / SOFTWARE DESCRIPTION

4.1 HARDWARE DESCRIPTION

4.1.1 Power Supply

Block diagram:

The ac voltage, typically 220v rms, is connected to a transformer, which steps that ac voltage down to the level of the desired dc output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation.

A regulator circuit removes the ripples and also remains the same dc value even if the input dc voltage varies, or the load connected to the output dc voltage changes. This voltage regulation is usually obtained using one of the popular voltage regulator IC units.

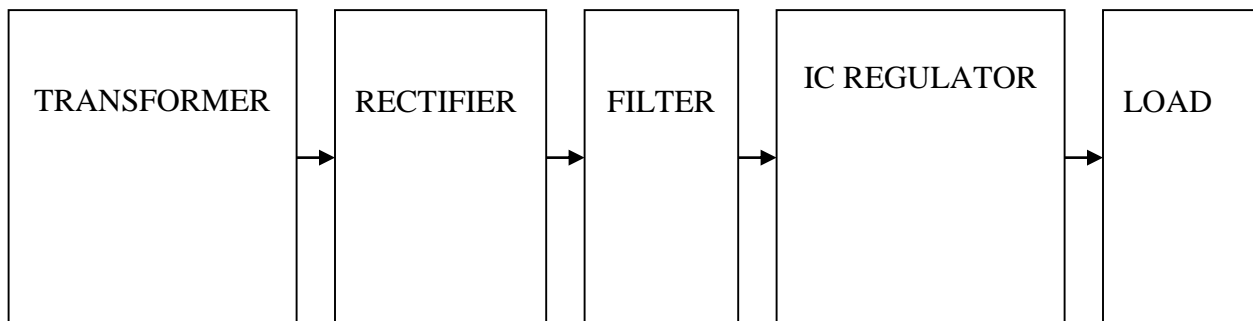


Figure.4.1.1: BLOCK DIAGRAM (Power Supply)

Working principle:

Transformer:

The potential transformer will step down the power supply voltage (0-230v) to (0-6v) level. Then the secondary of the potential transformer will be connected to the precision rectifier, which is constructed with the help of op-amp. The advantages of using precision rectifier are it will give peak voltage output as dc, rest of the circuits will give only rms output.

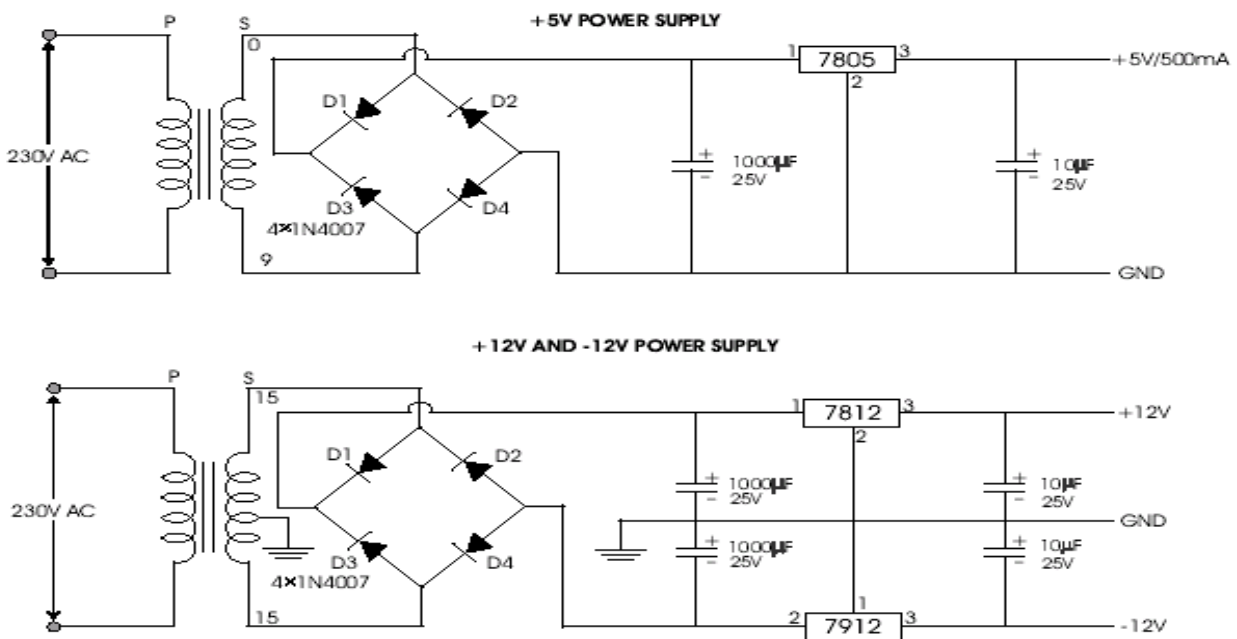


Figure.4.1.1.1: +5/+12V CIRCUIT DIAGRAM (Power Supply)

Bridge rectifier:

When four diodes are connected as shown in figure, the circuit is called as bridge rectifier. The input to the circuit is applied to the diagonally opposite corners of the network, and the output is taken from the remaining two corners.

Let us assume that the transformer is working properly and there is a positive potential, at point a and a negative potential at point b. The positive potential at point a will forward bias d3 and reverse bias d4.

The negative potential at point b will forward bias d1 and reverse d2. At this time d3 and d1 are forward biased and will allow current flow to pass through them; d4 and d2 are reverse biased and will block current flow.

The path for current flow is from point b through d1, up through rl, through d3, through the secondary of the transformer back to point b. This path is indicated by the solid arrows. Waveforms (1) and (2) can be observed across d1 and d3.

One-half cycle later the polarity across the secondary of the transformer reverse, forward biasing d2 and d4 and reverse biasing d1 and d3. Current flow will now be from point a through d4, up through rl, through d2, through the secondary of t1, and back to point a. This path is indicated by the broken arrows. Waveforms (3) and (4) can be observed across d2 and d4. The current flow through rl is always in the same direction. In flowing through rl this current develops a voltage corresponding to that shown waveform (5). Since current flows through the load (rl) during both half cycles of the applied voltage, this bridge rectifier is a full-wave rectifier.

One advantage of a bridge rectifier over a conventional full-wave rectifier is that with a given transformer the bridge rectifier produces a voltage output that is nearly twice that of the conventional full-wave circuit.

This may be shown by assigning values to some of the components shown in views a and b. Assume that the same transformer is used in both circuits. The peak voltage developed between points x and y is 1000 volts in both circuits. In the conventional full-wave circuit shown—in view a, the peak voltage from the center tap to either x or y is 500 volts. Since only one diode can conduct at any instant, the maximum voltage that can be rectified at any instant is 500 volts.

The maximum voltage that appears across the load resistor is nearly-but never exceeds-500 volts, as result of the small voltage drop across the diode. In the bridge rectifier shown in view b, the maximum voltage that can be rectified is the full

secondary voltage, which is 1000 volts. Therefore, the peak output voltage across the load resistor is nearly 1000 volts. With both circuits using the same transformer, the bridge rectifier circuit produces a higher output voltage than the conventional full-wave rectifier circuit.

IC voltage regulators:

Voltage regulators comprise a class of widely used ics. Regulator ic units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single ic. Ic units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustably set voltage. The regulators can be selected for operation with load currents from hundreds of mille amperes to tens of amperes, corresponding to power ratings from mille watts to tens of watts. A fixed three-terminal voltage regulator has an unregulated dc input voltage, v_i , applied to one input terminal, a regulated dc output voltage, from a second terminal, with the third terminal connected to ground.

The series 78 regulators provide fixed positive regulated voltages from 5 to 24 volts. Similarly, the series 79 regulators provide fixed negative regulated voltages from 5 to 24 volts.

- For ics, microcontroller, lcd ----- 5 volts
- For alarm circuit, op-amp, relay circuits ----- 12 volts

4.1.2 Microcontroller – Arduino UNO R3

A **microcontroller** (or **MCU** for *microcontroller unit*) is a small computer on a single integrated circuit. In modern terminology, it is a System on a chip or SoC. A microcontroller contains one or more CPUs (processor cores) along with memory and programmable input/output peripherals. Program memory in the form of Ferroelectric RAM, NOR flash or OTP ROM is also often included on chip, as well as a small amount of RAM. Microcontrollers are designed for embedded applications, in contrast to the microprocessors used in personal computers or other general-purpose applications consisting of various discrete chips.

The Arduino Uno is a microcontroller board based on the ATmega328. It has 20 digital input/output pins (of which 6 can be used as PWM outputs and 6 can be used as analog inputs), a 16 MHz resonator, a USB connection, a power jack, an in-circuit system programming (ICSP) header, and a reset button. It contains everything needed to support the microcontroller, simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features an ATmega16U2 programmed as a USB-to-serial converter. This auxiliary microcontroller has its own USB bootloader, which allows advanced users to reprogram it.

4.1.3 RFID – RC522

This is a Radio Frequency Identification (RFID) Transceiver. This is capable of writing reading and writing on the RFID tags, This RFID is used as an authentication device in the system. It consists of a master key card and number of RFID key tags where each key is unique 16-bit key Unicode for advance security.

4.1.4 Bluetooth – HC05-06

This is a standard Bluetooth module; this module is capable of sending and receiving packets. This is used as an authentication device in this system.

4.1.5 Servo Motors

Servomotors are controlled by means of pulse. These motors have been used for operating door locks and spray cans. They have the capability of rotating up to 180°. Two Servos are used in this proposed model, which are

SG-90 : Used for automated door lock.

V30003: Used for spraying can.

4.1.6 ODOR Sensor – MQ2/MQ3

This is a standard gas sensor MQ2, which detects the presence of butane or smoke in the air. This is used for the detection of LPG leakage or smoke in the air. Another one is MQ3, this is used to detect the presence of alcohol in the air, This is used as an authentication device in the proposed model.

4.1.7 GSM Module

This is a very low cost and simple Arduino GSM and GPRS module. It's the cheaper module now available in the market. This post will allow you to make Arduino controlled calls and also send text messages. This means the module supports communication in 900MHz band. We are from India and most of the mobile network providers in this country operate in the 900Mhz band. If you are from another country, you have to check the mobile network band in your area. A majority of United States mobile networks operate in 850Mhz band (the band is either 850Mhz or 1900Mhz). Canada operates primarily on 1900 MHz band. GSM modules are manufactured by different companies. They all have different input power supply specs. You need to double check your GSM modules power requirements.

4.2 SOFTWARE DESCRIPTION

4.2.1 C LANGUAGE

The C programming language is perhaps the most popular programming language for programming embedded systems. Most C programmers are spoiled because they program in environments where not only there is a standard library implementation, but there are frequently a number of other libraries available for use. The cold fact is, that in embedded systems, there rarely are many of the libraries that programmers have grown used to, but occasionally an embedded system might not have a complete standard library, if there is a standard library at all. Few embedded systems have capability for dynamic linking, so if standard library functions are to be available at all, they often need to be directly linked into the executable. Oftentimes, because of space concerns, it is not possible to link in an entire library file, and programmers are often forced to "brew their own" standard c library implementations if they want to use them at all. While some libraries are bulky and not well suited for use on microcontrollers, many development systems still include the standard libraries which are the most common for C programmers.

C remains a very popular language for micro-controller developers due to the code efficiency and reduced overhead and development time. C offers low-level control and is considered more readable than assembly. Many free C compilers are available for a wide variety of development platforms. The compilers are part of an IDEs with ICD support, breakpoints, single-stepping and an assembly window. The performance of C compilers has improved considerably in recent years, and they are claimed to be more or less as good as assembly, depending on who you ask. Most tools now offer options for customizing the compiler optimization. Additionally, using C increases portability, since C code can be compiled for different types of processor.

CHAPTER 5

SYSTEM DESIGN

5.1 STRUCTURE OF THE SYSTEM

The main objective of designing this system is to provide security for home and other locations. Security is the prime concern these days, so this system incorporates modules to secure the building from intruders and incase of fire accidents.

In this proposed model, we propose three-tier layer of security measures for any home or office situations. We consider three tiers, the tier 1 security concentrates in authenticating the genuine user to enter his/her house. The authentication is done using RFID tag where it is connected to an Servo motor for locking purpose and family members are given each a unique RFID card where there is an 16-bit key code each distinct from one other and still suffers from problems such as access RFID card losses. There is one master card for the main family person and remaining are all RFID tags, which are portable and used along with vehicle keychain. In case, of a guest user or loss of RFID tag we implemented a new tier, which authenticates genuine users.

In Tier 2, we developed an Android App (Three Tier Security) where guests can register their data in our database and the owner receives this information and grants permissions to their guests in case the owner is out of town or our relatives need to stay in our house while owner is away. This is done by Bluetooth module and where guest pair with the Bluetooth module and access the door unlock button he/she gains access to the house. Same goes for owner losing his/her RFID tag or master card can access his/her home by Android App for Admin (TTS Admin) this is used only by Owner and it connects with Bluetooth module of Arduino and authenticates access.

In Tier 3, this is worst-case scenario detection of intruders via odour sensor, this is experimental and has been implemented as way to find gas leakage or fire accidents in the house. Also used to find owner using unique smell stored on the module.

On the contrary, all these do the authentication process while an intruder is detected and to evade them out we used by spraying an non-fatal dose of Carbon Monoxide (CO) or Tear gas to lure them out. IR Camera used with app so, users can watch live video of their homes from anywhere. Also includes live monitoring of the house for the leakage of L.P.G gases, which may lead to fatal fire accidents. On detection of incidents like these, the users are informed with an alert message through sms via our android app. Through our prototyping system and real world experiments, we demonstrate this Three Tier Home Security using GSM Technology.

5.2 SYSTEM ARCHITECTURE

Here, main microcontroller used is Arduino UNO along with several modules. RFID Module (RFID MFRC522) is used along with servomotor (SG-90) for automatic door lock with REED switches used on the doors and windows. It consists of Master card and a RFID tags for authentication.

Next module is Bluetooth module where it is also used to unlock doors or windows for the user via android app. Experimental is odor sensor where we store particular persons smell where it detects that and allows them into his/her home. It also used to gas leakage that lead to fire accidents.

A GSM module (SIM-900A) is used for information of intruders or fire accidents alert. For precautions we used a servomotor (V3003) to control a spray can of non-fatal dose of CO or Tear gas. An IR Camera used with night vision, which can deliver very good quality to user via android app.

A Pin Diagram is made for further explanation where we find all modules connected to analog and digital pins of Arduino UNO.

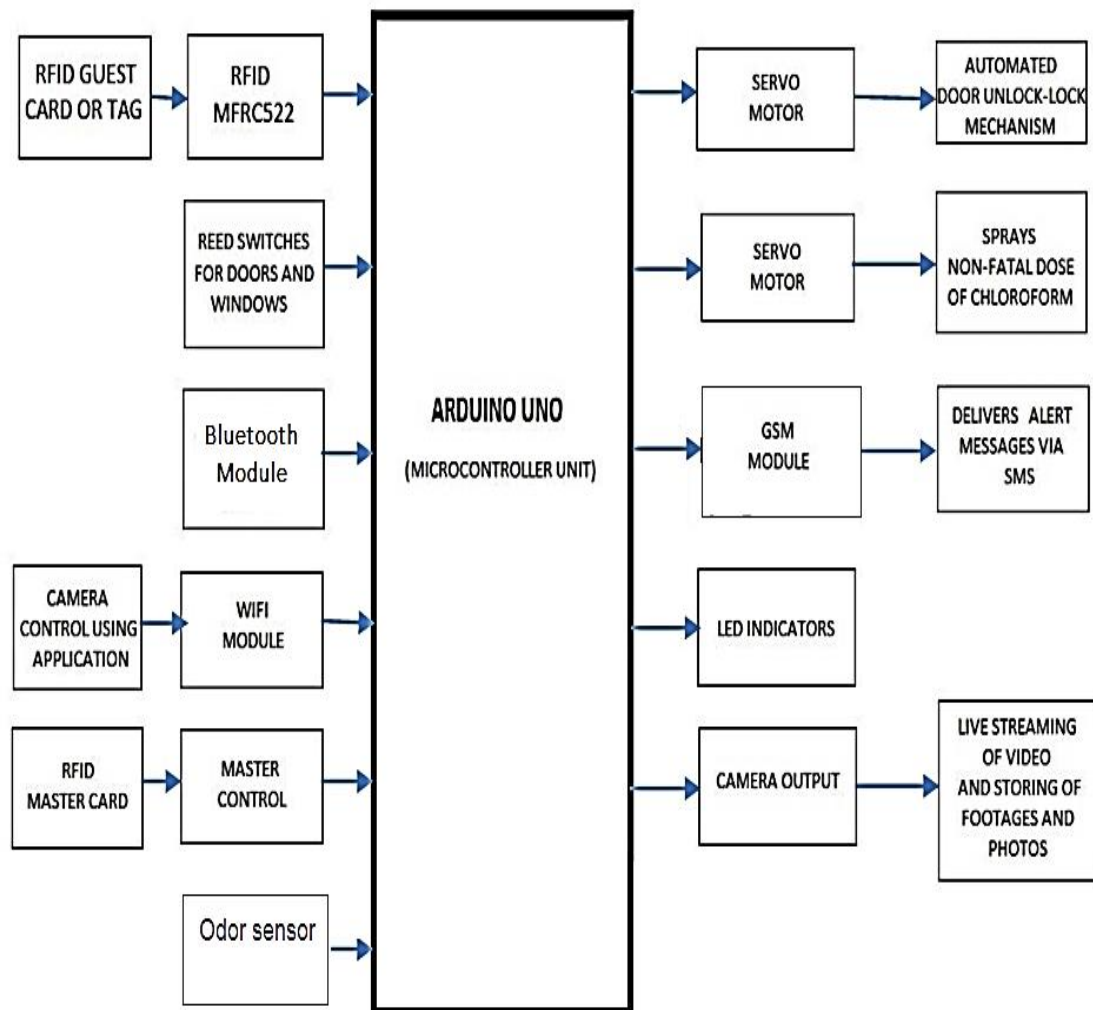


Figure 5.2.1 SYSTEM ARCHETECTURE

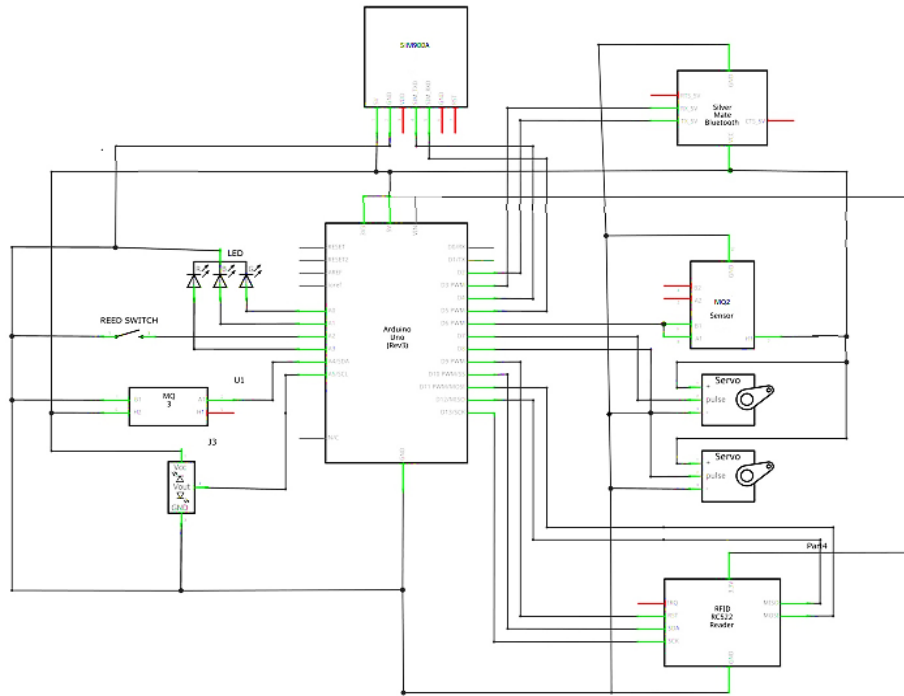


Figure 5.2.2 PIN DIAGRAM

5.3 MODULES

- RFID and Servo Motors Implementation
- Precautions in-case of Breach Access
- Odor Sensor Implementation

5.3.1 RFID and Servo Motors Implementation

In this phase, the users enter their homes by using automated door-lock, which is unlocked by using any of the three methods,

- Using RFID tag or Master Card.
- Using Android Application to authenticate via Bluetooth. The application has secure cloud login facility.
- In worst-case, when the user does not have RFID or Android facilities they can break the door and authentication is done based on their body smell

which is implemented as prototype in this model, upon successful authentication the door is unlocked using servomotor.

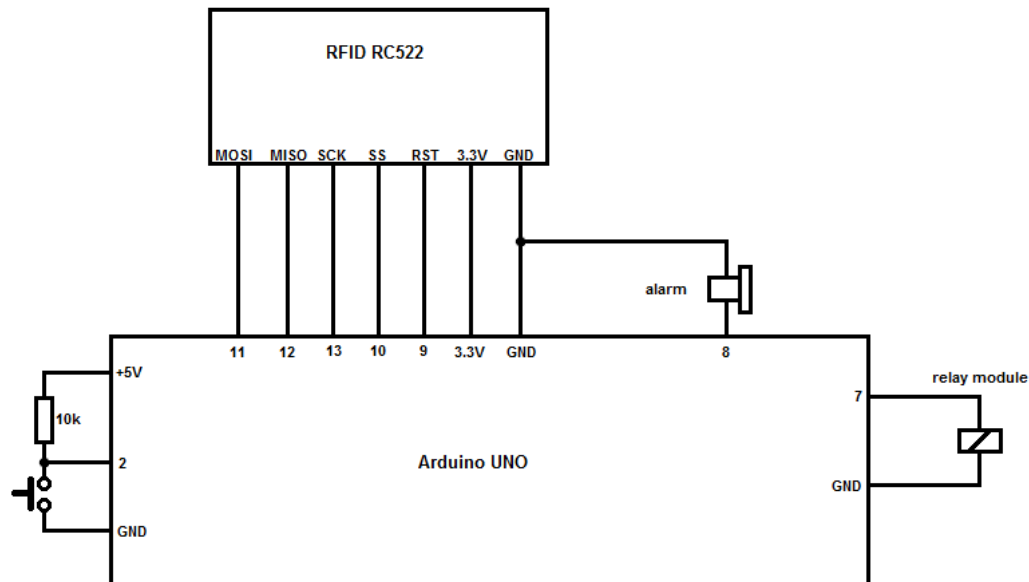


Figure 5.3.1 AUTHENTICATION AND DOOR LOCK

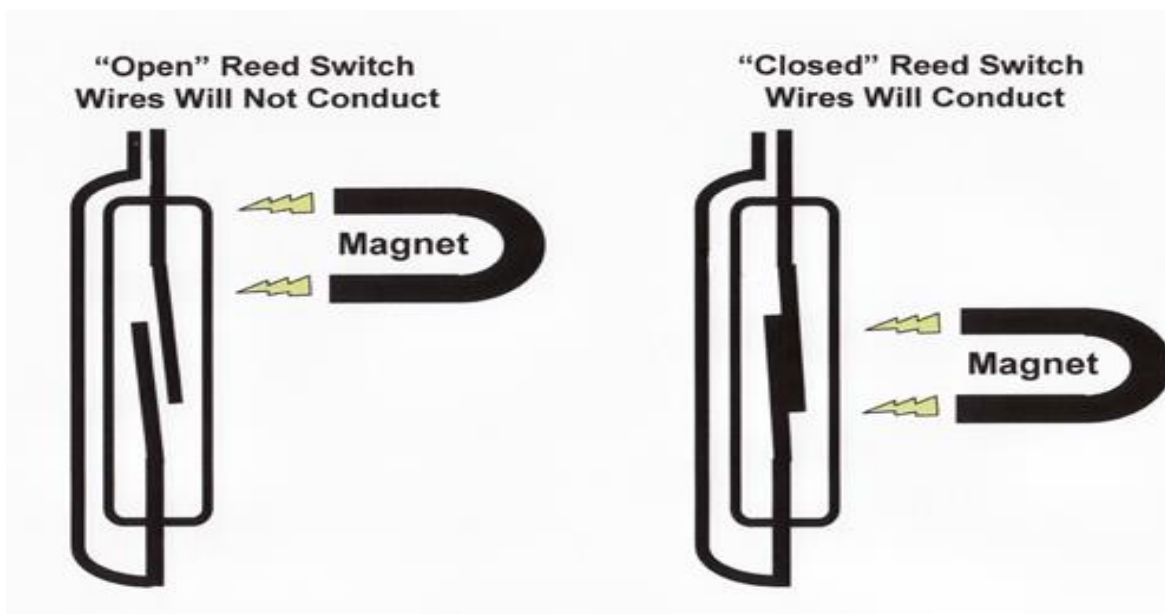


Figure 5.3.1.1 WORKING OF REED SWITCH

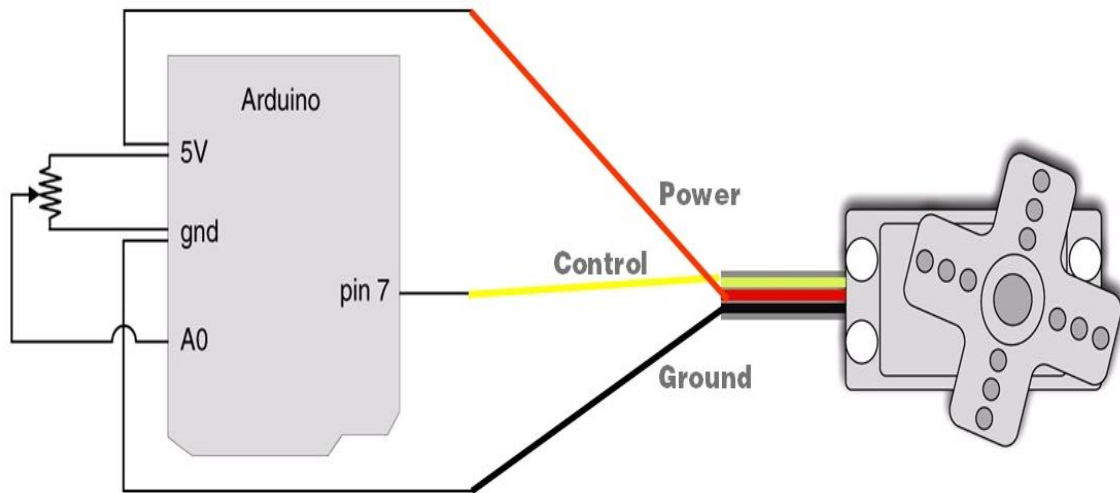


Figure 5.3.1.2 SERVO DIAGRAM

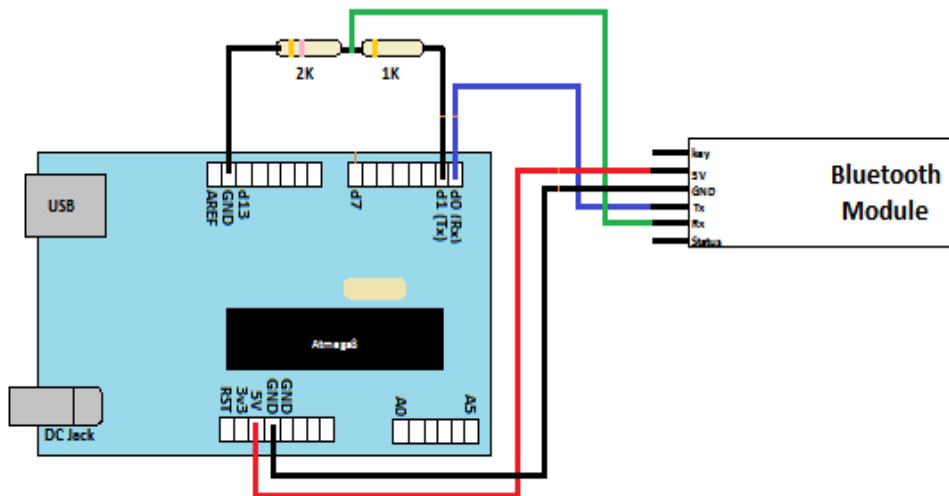


Figure 5.3.1.3 BLUETOOTH MODEL WORKING

5.3.2 Precautions In Case of Breach Access

In this phase in case of intruders, entering the home without authentication is considered as a breach. Therefore, with the help of IR sensor, Non-fatal dose of Carbon Monoxide or Tear gas is sprayed to evade the intruder out of the place. Simultaneously IR Camera module is used to capture photos of the intruder for the purpose of evidence.

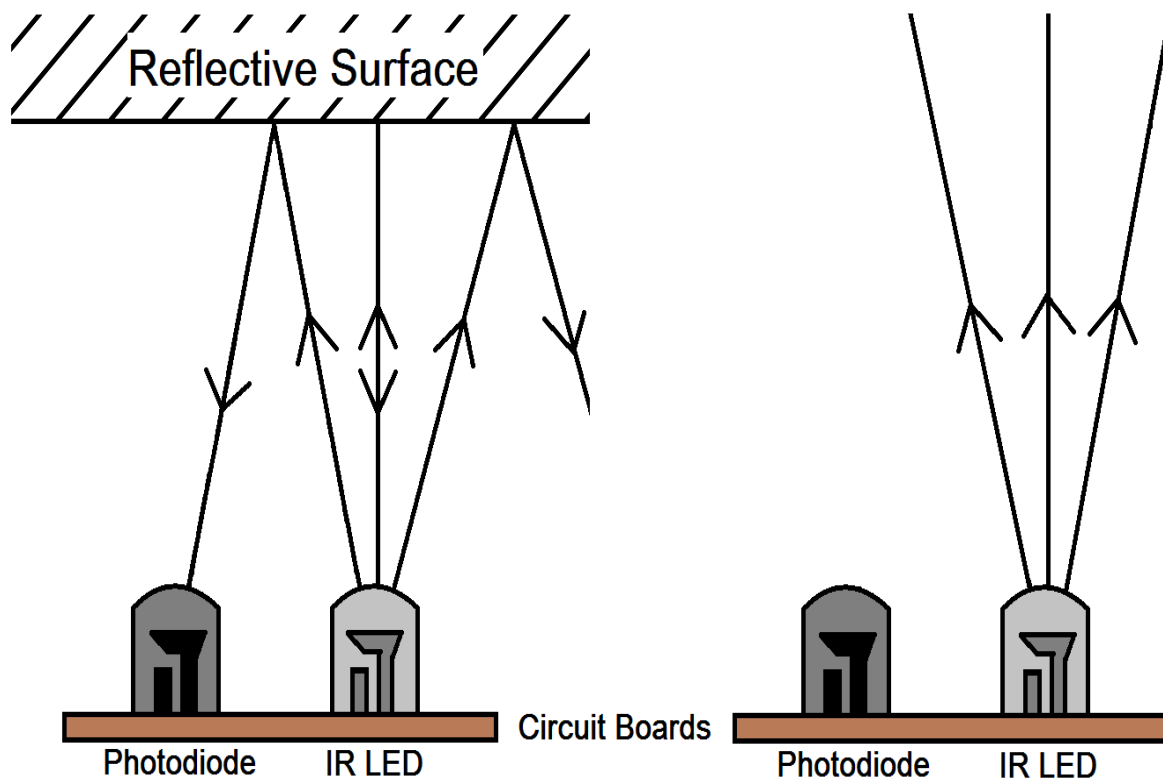


Figure 5.3.2 IR-SENSOR-ILLUSTRATION

5.3.3 Odor Sensor Implementation

In this phase the home is monitored for LPG leakage on detection of leakage or intrusion. The alarm is triggered on the user's phone with aid of GSM. In case of LPG gas leakage the main door of the house is automatically unlocked for emergency exit.

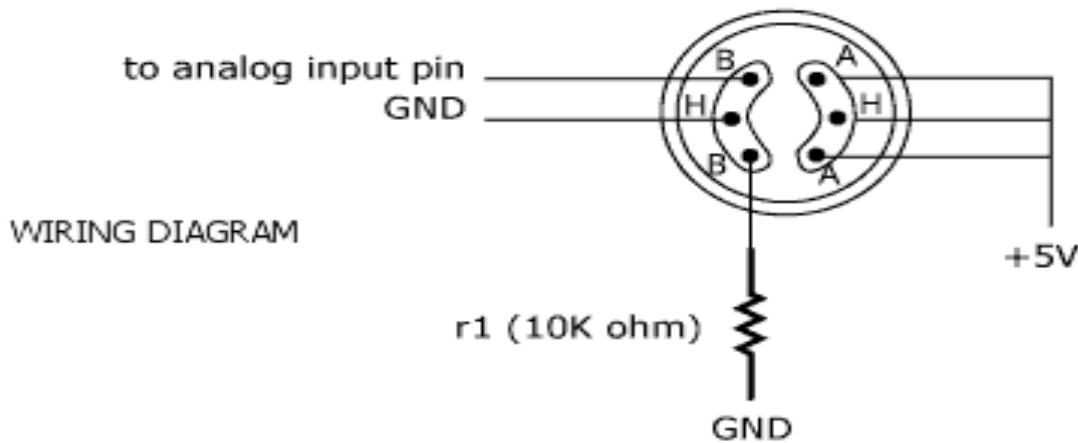


Figure 5.3.3 MQ2 AND MQ3 DIAGRAM

5.4 DATAFLOW DIAGRAM

A data-flow diagram (DFD) is a graphical representation of the “flow” of data through an information system. DFDs can also be used for the visualization of data processing (structured design). On a DFD, data items flow from an external data source or an internal data store to an internal data store or an external data sink, via an internal process.

A DFD provides no information about the timing or ordering of processes, or about whether processes will operate in sequence or in parallel. It is therefore quite different from a flowchart, which shows the flow of control through an algorithm, allowing a reader to determine what operations will be performed, in what order, and under what circumstances, but not what kinds of data will be input to and output from the system, nor where the data will come from and go to, nor where the data will be stored (all of which are shown on a DFD).

a) Level 0

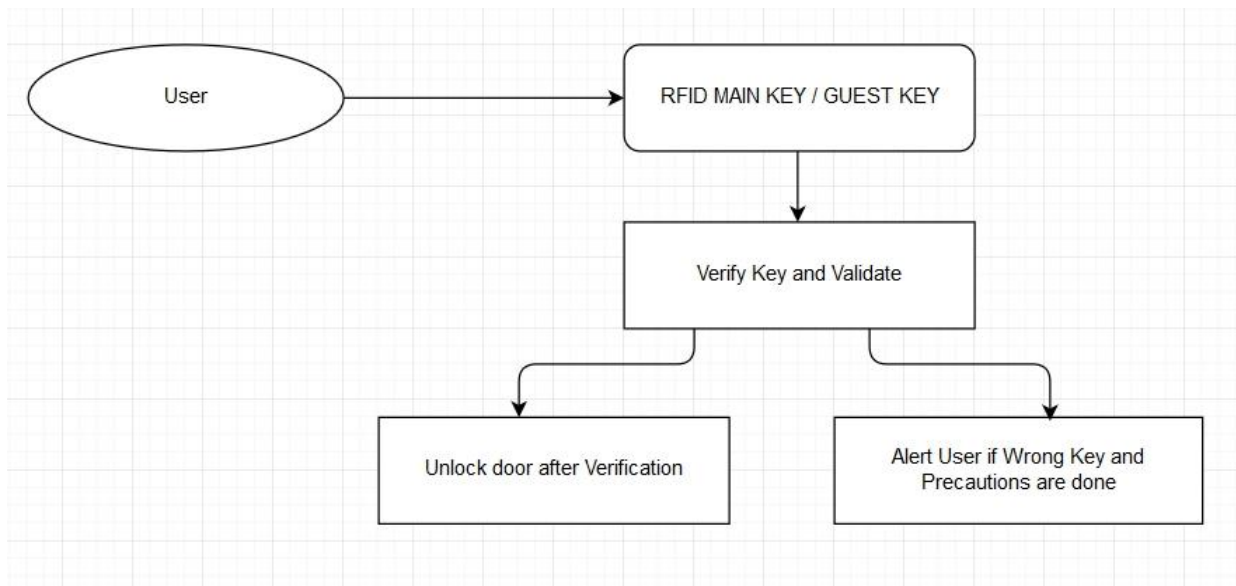


Figure 5.4.1 LEVEL 0 DATA FLOW DIAGRAM

b) Level 1

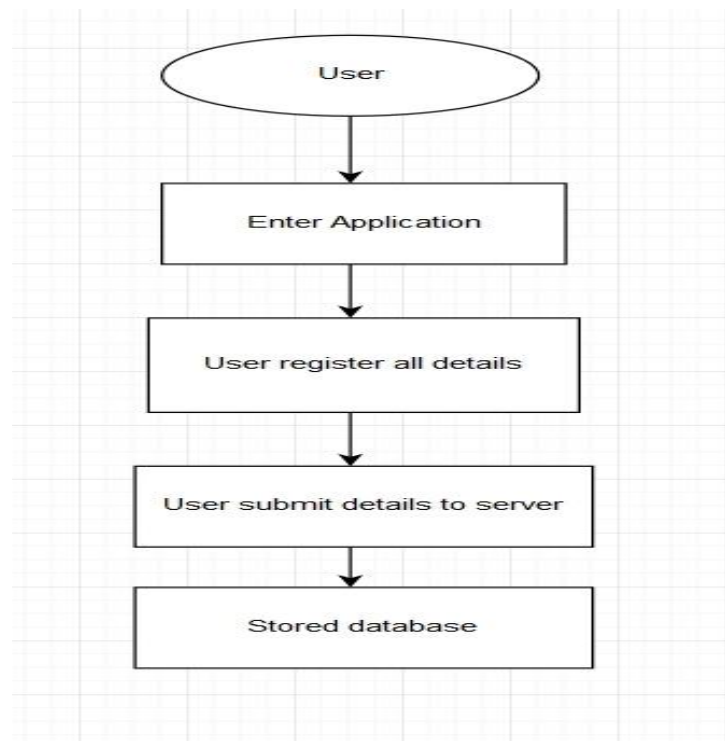


Figure 5.4.2 LEVEL 1 DATA FLOW DIAGRAM

c) Level 2

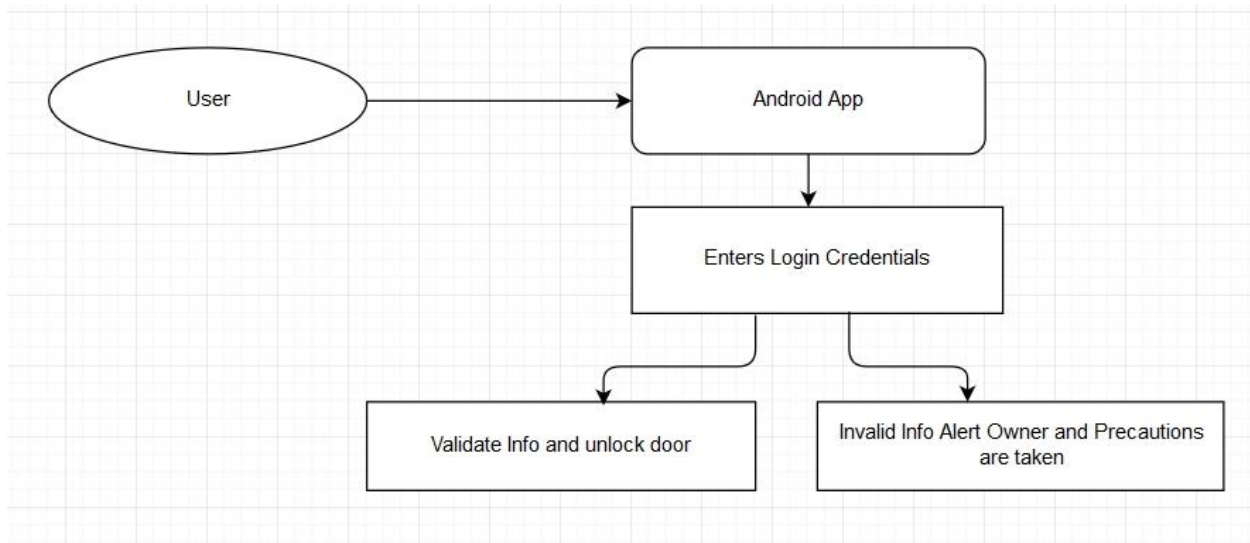


Figure 5.4.3 LEVEL 2 DATA FLOW DIAGRAM

5.5 UML DIAGRAM

5.5.1 Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. The following figure no.5.1 shows the use case diagram of the overall working system.

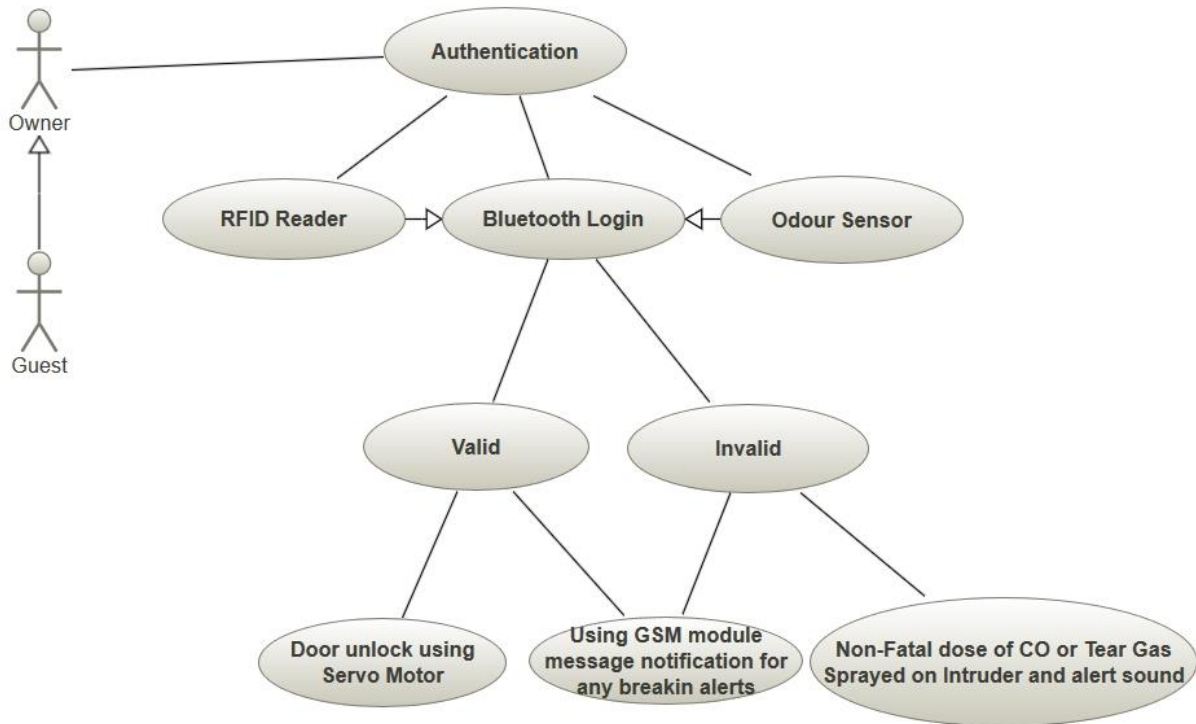


Figure 5.5.1 USE CASE DIAGRAM

5.5.2 Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational systematic workflow of components in a system. An activity diagram in figure 5.2 shows flow of control.

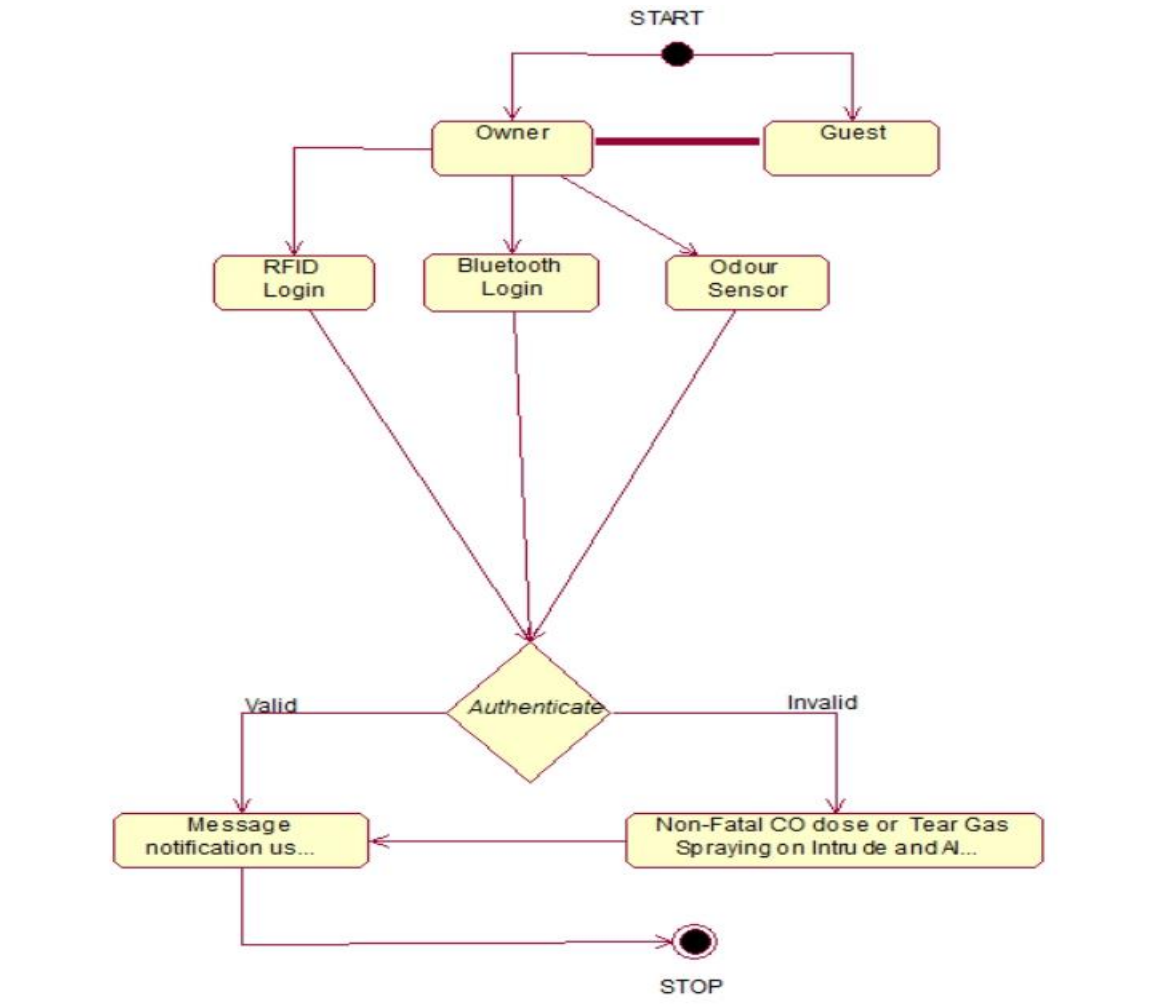


Figure 5.5.2 ACTIVITY DIAGRAM

5.5.3 Sequence Diagram

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called Event-trace diagrams, event scenarios, and timing diagrams.

A sequence diagram shows, as parallel vertical lines (lifelines), different processes or object that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in they occur. This allows the specification of

simple runtime scenarios in a graphical manner. The following figure illustrates the overall working of the sensor.

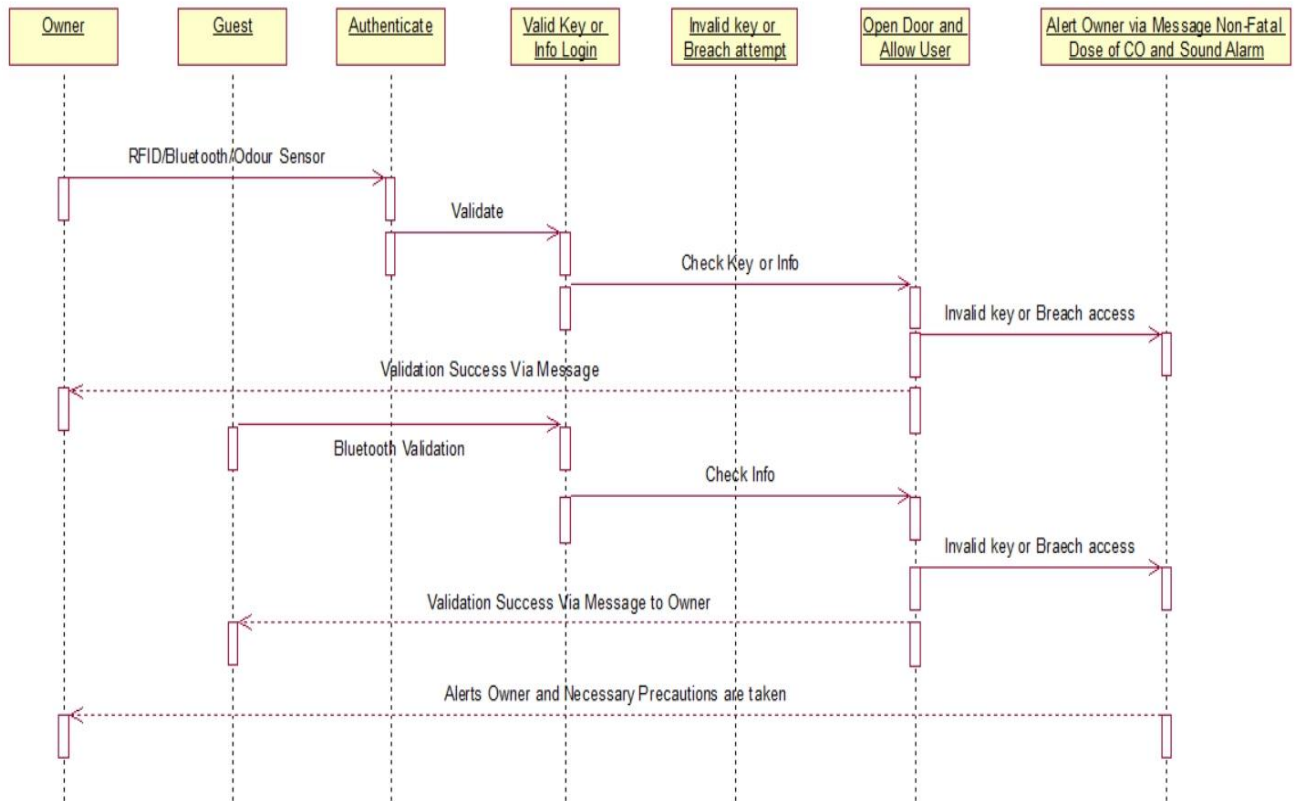


Figure 5.5.3 SEQUENCE DIAGRAM

5.5.4 Collaboration Diagram

Collaboration Diagram belong to group of UML, diagrams called Interactions Diagrams. Collaboration diagrams, like Sequence Diagrams, show how objects interact over the course of time. However, instead of showing the sequence of events by the layout on the diagrams, collaboration diagrams show the sequence by numbering the messages on the diagram. This makes it easier to show how the objects are linked together, but harder to see the sequence at a glance. The following figure gives the collaboration diagram of the entire working of the system.

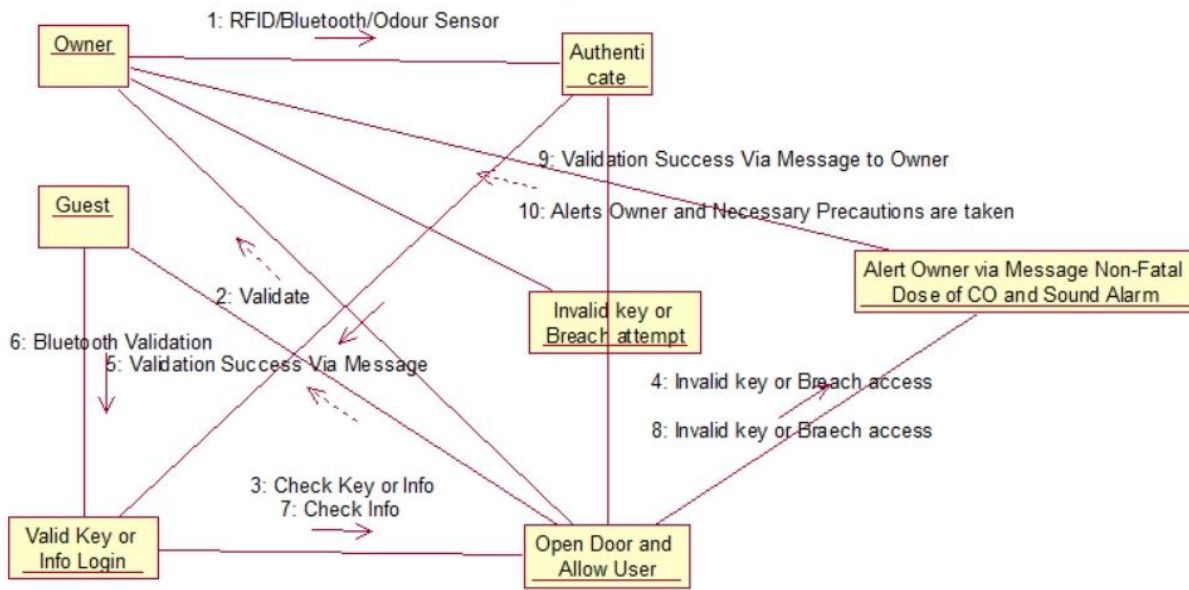


Figure 5.5.4 COLLABORATION DIAGRAM

CHAPTER 6

CONCLUSION

In this paper, we propose a dynamic proposed system presents design and implementation of a smart home security system based on microcontroller along with GSM for user-friendly application. The system is intelligent enough to monitor the secure environment. In addition, the user is informed about the security breach through GSM network that provides a special opportunity whenever the user stays at far away from home. However, Android application is the most stunning feature in order to control the system through a wireless device. Moreover, the system provides the reliable operation within reasonable cost and removes the system complexity. In this work, traditional burglar alarm mode, LED lights and are the promising features used to ensure reliability. The whole system is implemented on a practical home security system, which requires considerable effort to install it. Consequently, the system is also applicable for commercial purposes due to versatile ways of security and controllability.

APPENDIX-1

SAMPLE CODE

```
#include <AddicoreRFID.h>
#include <SPI.h>
#include<Servo.h>
#include<SoftwareSerial.h>
#define uchar unsigned char
#define uint unsigned int
uchar fifobytes;
uchar fifoValue;
int bluetoothTx=2;
int bluetoothRx=3;
int gsmTx=4;
int gsmRx=5;
int mq3value1,mq3value2,mq3value3,mq3value4;
SoftwareSerial bluetooth(bluetoothTx,bluetoothRx);
SoftwareSerial gsm(gsmTx,gsmRx);
AddicoreRFID myRFID;
const int chipSelectPin = 10;
const int NRSTPD = 9;
const int spin=8;
const int spin2=7;
const int mq2=6;
char msg1[]={ "tts_guest_user" };
char msg2[]={ "authenticated_access" };
char alert1[]={ "tts_home_alert" };
char alert2[]={ "tts_home_fire" };
```

```

int mq2value;
Servo s,s0;
#define MAX_LEN 16
void setup() {
  Serial.begin(9600);
  delay(100);
  s.attach(spin);
  s0.attach(spin2);
  SPI.begin();
  pinMode(A0,OUTPUT);
  pinMode(A1,OUTPUT);
  pinMode(A2,INPUT);
  pinMode(A3,OUTPUT);
  pinMode(A4,INPUT);
  pinMode(A5,INPUT);
  pinMode(mq2,INPUT);
  digitalWrite(A2,HIGH);
  pinMode(chipSelectPin,OUTPUT);
  digitalWrite(chipSelectPin, LOW);
  pinMode(NRSTPD,OUTPUT);
  digitalWrite(NRSTPD, HIGH);
  myRFID.AddicoreRFID_Init();
}
void loop()
{
  bluetooth.begin(9600);
  mq2value=analogRead(A2);

```

```

if(mq2value<100)
{
    sendSMS(alert2);
    s.write(180);
    for(;;mq2value>220;)
    {
        digitalWrite(A0, HIGH);
        digitalWrite(A1, HIGH);
        digitalWrite(A3, HIGH);
        delay(1000);
        digitalWrite(A0, LOW);
        digitalWrite(A1, LOW);
        digitalWrite(A3, LOW);
        mq2value=analogRead(A2);
    }
    s.write(0);
    bluetooth.end();
}
uchar i, tmp, checksum1;
uchar status;
bool b=false;
s.write(0);
    if(bluetooth.available()> 0 )
    {
        int servopos = bluetooth.read();
        if(servopos==0)
            s.write(0);
    }

```

```

else if(servopos==180)
{
    Serial.println(servopos);
    b=true;
    digitalWrite(A0, HIGH);
    delay(500);
    digitalWrite(A0, LOW);
    delay(500);
    digitalWrite(A0, HIGH);
    delay(500);
    digitalWrite(A0, LOW);
    delay(500);
    digitalWrite(A0, HIGH);
    delay(500);
    digitalWrite(A0, LOW);
    s.write(180);
    digitalWrite(A0, HIGH);
    s.write(180);
    sendSMS(msg1);
    delay(4000*2);
    if(digitalRead(mq2)==LOW)
    {
        s.write(0);
        digitalWrite(A0, LOW);
    }
}
Serial.println(servopos);

```

```

}

uchar str[MAX_LEN];
uchar RC_size;
uchar blockAddr;
String mynum = "";
str[1] = 0x4400;
status = myRFID.AddicoreRFID_Request(PICC_REQIDL, str);
if (status == MI_OK)
{
    Serial.println("RFID tag detected");
    Serial.print("Tag Type:\t\t");
    uint tagType = str[0] << 8;
    tagType = tagType + str[1];
    switch (tagType) {
        case 0x4400:
            Serial.println("Mifare UltraLight");
            break;
        case 0x400:
            Serial.println("Mifare One (S50)");
            break;
        case 0x200:
            Serial.println("Mifare One (S70)");
            break;
        case 0x800:
            Serial.println("Mifare Pro (X)");
            break;
    }
}

```

```

        case 0x4403:
            Serial.println("Mifare DESFire");
            break;
        default:
            Serial.println("Unknown");
            break;
    }
}

status = myRFID.AddicoreRFID_Anticoll(str);
if (status == MI_OK)
{
    checksum1 = str[0] ^ str[1] ^ str[2] ^ str[3];
    Serial.print("The tag's number is:\t");
    Serial.print(str[0]);
    Serial.print(" , ");
    Serial.print(str[1]);
    Serial.print(" , ");
    Serial.print(str[2]);
    Serial.print(" , ");
    Serial.println(str[3]);

    Serial.print("Read Checksum:\t\t");
    Serial.println(str[4]);
    Serial.print("Calculated Checksum:\t");
    Serial.println(checksum1);
    if(str[0] == 38 && str[1]==159 && str[2]==45 && str[3]==43)
    {

```



```

digitalWrite(A0, HIGH);
delay(500);
digitalWrite(A0, LOW);
delay(500);
digitalWrite(A0, HIGH);
delay(500);
digitalWrite(A0, LOW);
delay(500);
digitalWrite(A0, HIGH);
delay(500);
digitalWrite(A0, LOW);
s.write(180);
digitalWrite(A0, HIGH);
sendSMS(msg1);
delay(3000*2);
if(digitalRead(mq2)==LOW)
{
    s.write(0);
    digitalWrite(A0, LOW);
}
b=true;
Serial.println("\nHello Guest!\n");
}
else if(str[0] == 181&&str[1]==218&&str[2]==218&&str[3]==82)
{
    digitalWrite(A1, HIGH);
    delay(500);

```

```

    digitalWrite(A1, LOW);
    delay(500);
    digitalWrite(A1, HIGH);
    delay(500);
    digitalWrite(A1, LOW);
    delay(500);
    digitalWrite(A1, HIGH);
    delay(500);
    digitalWrite(A1, LOW);
    s.write(180);
    digitalWrite(A1, HIGH);
    delay(5000*2);
    if(digitalRead(mq2)==LOW)
    {
        s.write(0);
        digitalWrite(A1, LOW);
    }
    b=true;
    Serial.println("\nHello ADMIN!\n");
}
else
{
    Serial.println("Unknown card");
    digitalWrite(A3, HIGH);
    delay(5000);
    digitalWrite(A3, LOW);
}

```

```

Serial.println();
delay(1000);
}

myRFID.AddicoreRFID_Halt();
if(digitalRead(mq2)==HIGH&&b==false)
{
mq3value1=analogRead(A4);
delay(500);
mq3value2=analogRead(A4);
delay(500);
for(;digitalRead(A5)==LOW&&digitalRead(mq2)==HIGH;);
mq3value3=analogRead(A4);
delay(500);
mq3value4=analogRead(A4);
Serial.print("Odour Value 1:");Serial.println(mq3value1);
Serial.print("Odour Value 2:");Serial.println(mq3value2);
Serial.print("Odour Value 3:");Serial.println(mq3value3);
Serial.print("Odour Value 4:");Serial.println(mq3value4);

if(mq3value1<310&&mq3value2<310&&mq3value3<310&&mq3value4<310)
{
digitalWrite(A3, HIGH);
s0.write(180);
delay(1000);
s0.write(0);
sendSMS(alert1);
digitalWrite(A3, LOW);

```

```

    }
    else
    {
        sendSMS(msg2);
        for(;digitalRead(A5)==HIGH;);
    } }
    if(digitalRead(mq2)==HIGH&&b==true)
    {
        for(;digitalRead(mq2)==HIGH;);
        digitalWrite(A0, HIGH);
        sendSMS(msg1);
        digitalWrite(A0, LOW);
    } }

void sendSMS(char message[30])
{
    gsm.begin(9600);
    delay(1000);
    gsm.println("AT+CMGF=1");
    delay(1000);
    gsm.println("AT+CMGS=\"+917845639909\\r\"");
    delay(1000);
    gsm.println(message);
    delay(100);
    gsm.println((char)26);
    delay(1000);
    gsm.end();
}

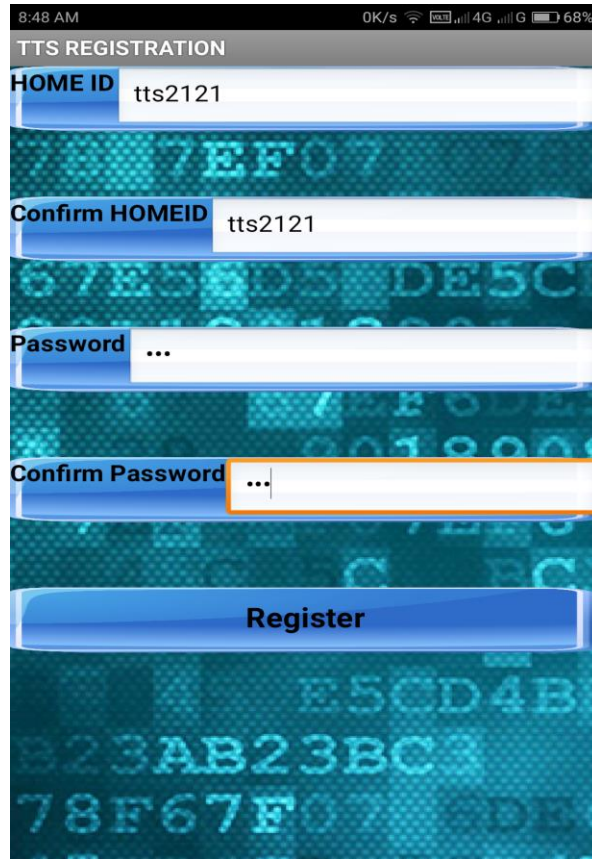
```

APPENDIX-2

SCREENSHOTS

1. Registration

The initial registration procedure is shown.



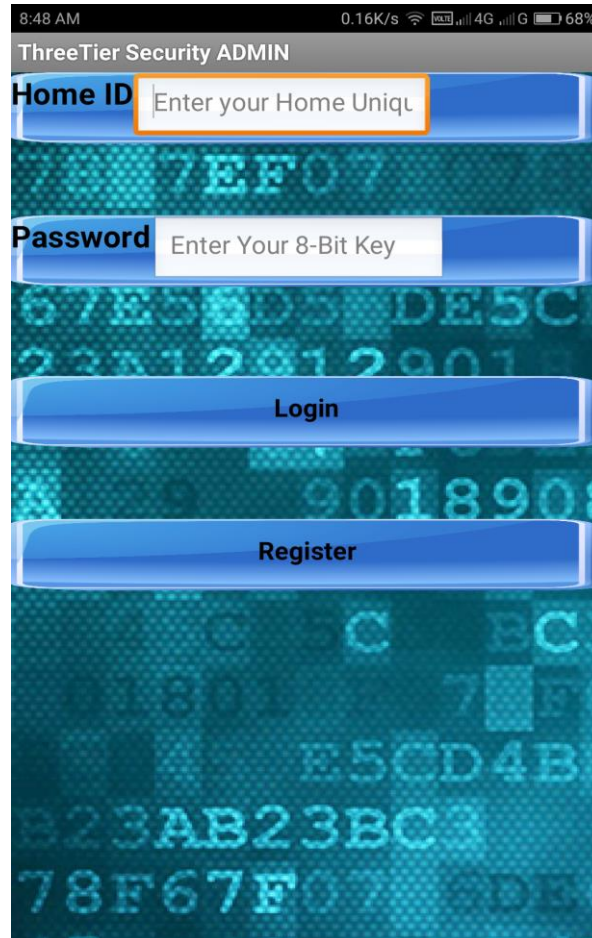
The screenshot shows a mobile application interface for "TTS REGISTRATION". The background is a dark blue grid with faint, light blue hexadecimal characters. The form consists of several input fields and a button:

- HOME ID**: A text input field containing the value "tts2121".
- Confirm HOMEID**: A text input field containing the value "tts2121".
- Password**: A text input field with masked characters represented by three dots "...".
- Confirm Password**: A text input field with masked characters represented by three dots "...". This field is highlighted with an orange border.
- Register**: A blue button with white text, located at the bottom of the form.

The status bar at the top of the screen displays the time "8:48 AM", network status "0K/s", signal strength, "4G", and battery level "68%".

2. Login

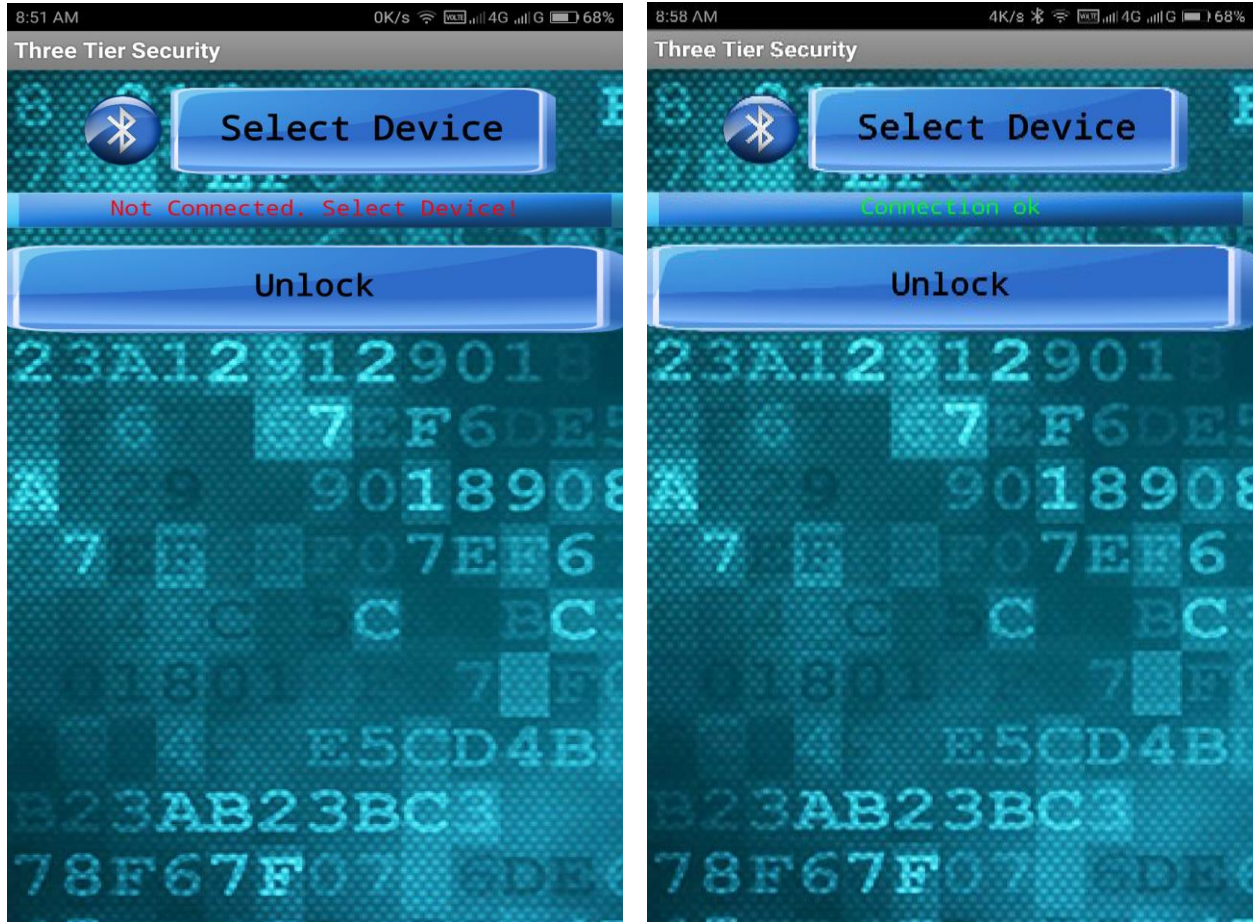
The login page is displayed. This allows initial login.



The screenshot shows a mobile application interface for 'ThreeTier Security ADMIN'. At the top, the status bar displays '8:48 AM', '0.16K/s', and a 68% battery level. The app title 'ThreeTier Security ADMIN' is centered at the top. Below it, there are two input fields: 'Home ID' with the placeholder text 'Enter your Home Uniqu' and 'Password' with the placeholder text 'Enter Your 8-Bit Key'. The 'Home ID' field is highlighted with an orange border. Below the input fields are two blue buttons: 'Login' and 'Register'. The background of the app is a dark blue with a pattern of glowing green hexadecimal characters.

3. Bluetooth Pairing

This allows a list of devices which pairs with the Bluetooth module.



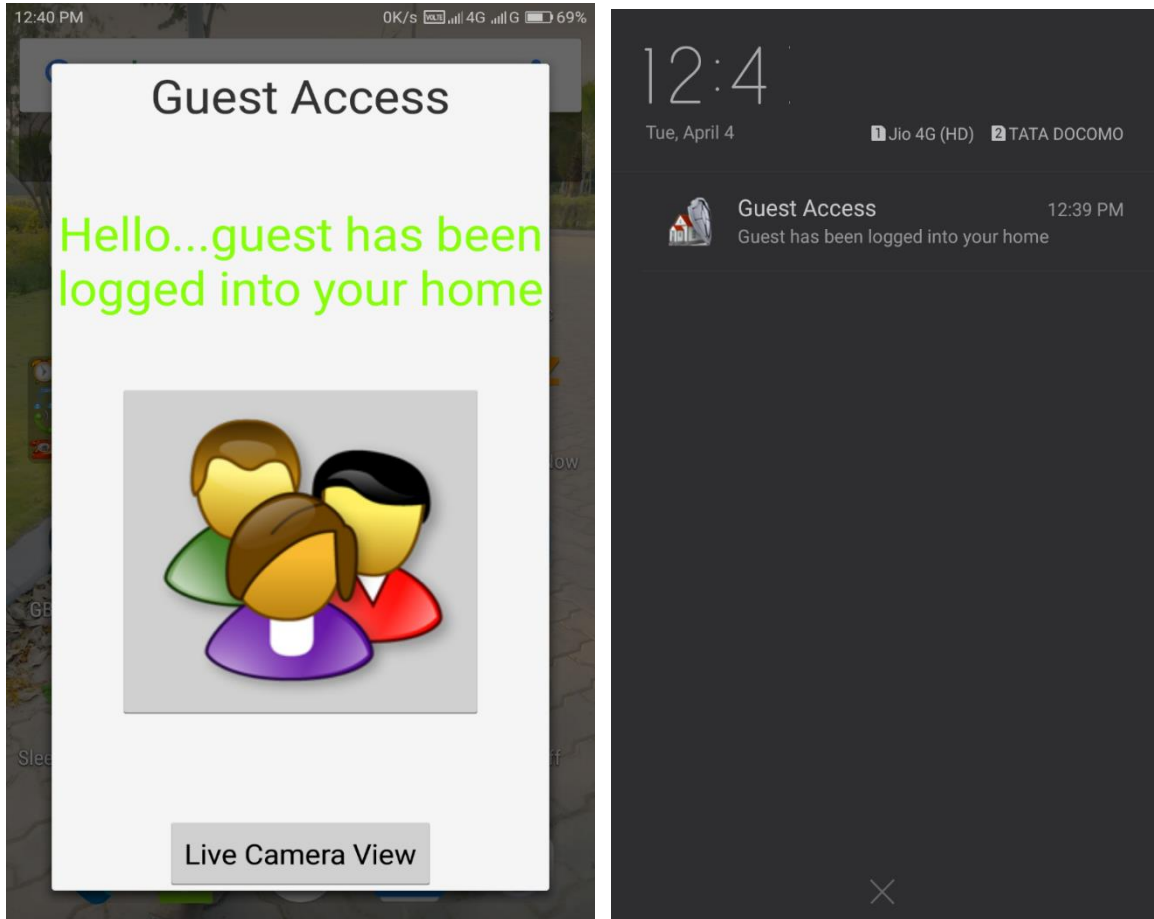
4. Alert Messages

This shows alert messages received to the user when a breach attempt or in case of fire accident.



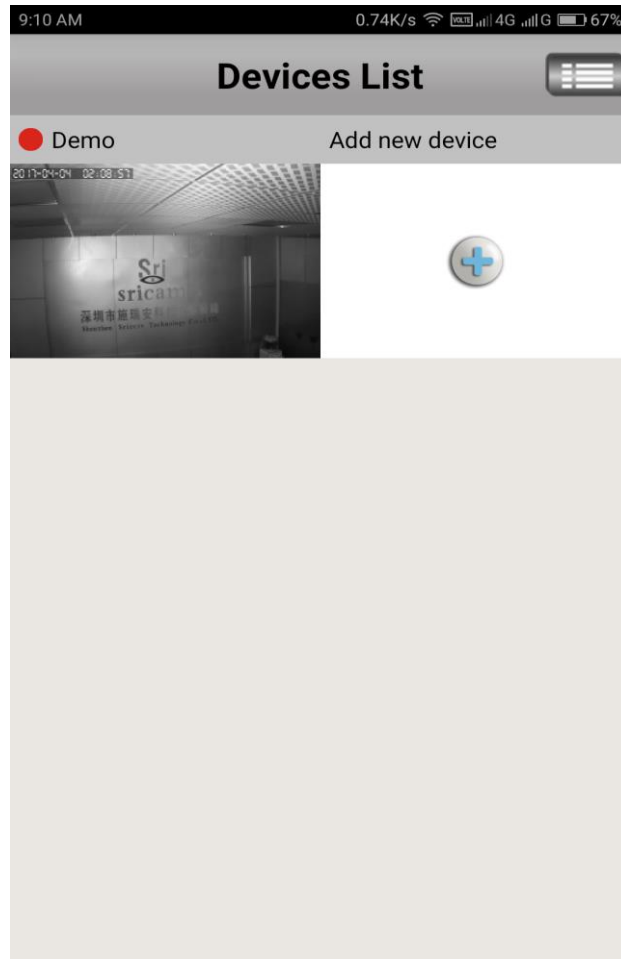
5. Guest User Login

This shows what happens when a guest logs in and the user receiver's notification message.



6. Live Camera Feed

This shows live camera feed to user device via internet.



REFERENCES

- [1] Abhishek S. Parab (2015), 'Implementation of Home Security System using GSM module and Microcontroller', International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2950-2953.
- [2] Anandan R, Karthik B, Kiran Kumar Dr.T.V.U (2015), 'Wireless Home And Industrial Automation Security System Using Gsm', Journal of Global Research in Computer Science, Vol. 4 (4), 55-59.
- [3] Chintaiah N, Rajasekhar K, Dhanraj V (2011), 'Automated Advanced Industrial and Home Security Using GSM and FPGA', International Journal of Computer Science and Information Technologies, Vol.2 (4), 1598-1602.
- [4] Jayashri Bangali and Arvind Shaligram (2013), 'Design and Implementation of Security Systems for Smart Home based on GSM technology', International Journal of Smart Home, Vol. 7 (6), 201-208.
- [5] Raqibull Hasan, Mohammad Monirujjaman Khan, Asaduzzaman Ashek, Israt Jahan Rumpa (2015), 'Microcontroller Based Home Security System with GSM Technology', Open Journal of Safety Science and Technology, Vol. 5, 55-62.

WEB REFERENCE

- 1. <https://create.arduino.cc/projecthub/Aritro/security-access-using-rfid-reader>
- 2. <http://www.instructables.com/id/Magnetic-Door-Sensor-and-Arduino>
- 3. <https://create.arduino.cc/projecthub/Aritro/smoke-detection-using-mq-2-gas-sensor-79c54a>
- 4. <http://www.instructables.com/id/Arduin-Adroid-USB-Serial-Communication/>