Revolutionizing Home Security

Mihir Upagade, Jaideep Dongare, Anshul Ajapuje, Uttakarsh Panse & Rohan Kamble
Guided by Dr.Vaishnavi Ganesh
Department of Computer Science And Engineering , Priyadarshani College of Engineering ,Rashtrasant Tukdoji Maharaj Nagpur University

ABSTRACT

We are currently experiencing the fourth industrial revolution, with technology rapidly advancing and making our lives more comfortable and efficient. The Internet of Things (IoT) is a significant contributor to this revolution. One of the key areas of IoT is smart home systems, or home automation, which is becoming increasingly popular in improving our quality of life. In this project, we introduce an IoT-based, low-cost smart electrical equipment automation system. The system is controlled via a web portal, which is connected to an ESP32 Wi-Fi module. A custom-made private web server is developed to maintain the current states of electrical appliances, enabling users to control their devices remotely.

KEYWORDS: ESP32 Cam , IOT, Web Server , Adaptor.

1. INTRODUCTION

The use of the Internet of Things (IoT) is rapidly expanding across various fields, including industries, offices, education institutions, and homes. With IoT, every physical object can be connected to the internet and controlled and monitored remotely. One of the key advantages of IoT is its ability to automate electrical devices, which is becoming increasingly popular with the advent of voice recognition software like Amazon Alexa. In this project, we aim to develop a low-cost and energy-efficient IoT-based system that can transform pre-existing electrical devices into smart devices. The system will enable users to control and monitor their electrical appliances remotely from anywhere and at any time. We will focus on developing an Electrical Load Control System (ELCS) that can be controlled wirelessly using IoT techniques. With the growing demand for wireless systems in the market, our project aims to provide a cost-effective solution that can be used in homes and other settings.

The world is rapidly advancing towards an era of the Internet, where every physical object can be connected and communicated through the internet. According to research, the number of Internet of Things (IoT) connected devices installed worldwide is expected to reach 75.44 billion between 2015 to 2025. With the rise of voice recognition software such as Amazon Alexa, there is an increasing demand for automation of electrical devices. Our main objective is to develop an efficient and affordable way to transform existing electrical devices into smart electrical devices.

To achieve this, we propose a low-cost, low power consumption IoT-based system that allows registered users to control and monitor their electrical appliances from anywhere at any time. The system utilizes an Electrical Load Control System (ELCS) that can be remotely controlled through a wireless IoT network. IoT is a revolutionary idea that is transforming every field, including industries, offices, educational institutions, and homes.

Our system aims to provide a wireless solution that enables users to control their electrical equipment remotely, eliminating the need for physical control. This IoT-based solution offers flexibility and convenience, making it easy for users to monitor and control their electrical appliances from anywhere at any time. By utilizing IoT techniques, our system can be implemented in a wide range of applications, including homes, offices, industries, and educational institutions, among others.

Introduction to Integrated systems

Integrated systems are specialized electronic devices that utilize microprocessors or microcontrollers for their implementation. These systems are designed to perform specific tasks and are integrated within a hardware device.

The use of microprocessors in these devices provides flexibility and simplifies the design process, allowing for easier bug fixes, modifications, or new feature additions by simply updating the controlling software.

Integrated systems are typically designed to perform a single function and are tightly constrained in terms of their size, cost, power consumption, and performance metrics. These systems can be classified into four categories: Stand-alone integrated systems, Real-time integrated systems, Network Information Appliances, and Mobile Devices. Integrated systems designers must have a good understanding of hardware technologies and use specific programming languages and software to develop and manipulate the equipment.

The development of integrated systems can be expensive due to the necessary development time and built-in efficiencies. However, they are highly valued in specific industries for their reliability, efficiency, and speed.

Characteristics of Integrated Systems

Single-functioned – Integrated systems perform specialized operations and are designed for a specific task that cannot be altered without physically manipulating the circuitry.
Tightly constrained – Integrated systems have tight design constraints, including size, cost, power consumption, and performance metrics, which must be met to ensure optimal operation.
Reactive and real-time – Many integrated systems must continually react to changes in the system's environment and must compute certain results in real-time without any delay.
Microprocessor-based – Integrated systems use microprocessors or microcontrollers for their implementation.
Memory – Integrated systems have embedded software that is stored in ROM, and they usually do not require secondary memories.
Connected – Integrated systems have connected peripherals to connect input and output devices. A combination of hardware and software is used to provide flexibility, performance, and security.

2. REVIEW OF LITERATURE

In the IoT platform-based home security system, the main emphasis on protecting our loved ones and our belongings at home. Today numbers of IoT based home security systems are available in market. According to the literature and market survey, the common parameters of IoT enabled home security system are 24 hours monitoring and detection of the intruder, real time, cost effective and precise notification system suggested by various researchers. Following are the contributions of various researcher done in IoT domain [6].

Rani et al. (2018) explains the IoT based home security using Raspberry Pi which give SMS alert to authorize person through WAY2SMS and image of the unauthorized person via g-mail.

Dinakar et al. (2018) proposed IoT based automated home security system using Raspberry Pi which gives intruder detection alarm and notification to the owner.

Ghodke et al. (2017) explains in their paper how the IoT network-based system send the information of any person image coming close to the door for home security to the owner.

Anwar et al. (2016) explains the IoT based door accessibility and voice alerting through smart phone for home security system.

Tanaya and Kishore (2016) explains the up-gradation of home security system with face detection technique using haar algorithm in open CV for the detection of authorized or design and build unauthorized person.

Chowdhury et al. (2013) describes IoT based remote access control system for authorized person at door using raspberry Pi.

In [1] the author has come up with the technology for home automation and security by using a Bluetooth based system. The home appliances that are to be controlled are connected to the input/output ports of the Arduino BT board via relays. Passwords are provided for the purpose of protection so that only the authorized users can

access the home appliances. The python script is used for programming purpose as it is portable and can run on any platform. A feedback circuit is used to indicate the status of the home appliances after receiving a command from the phone. The disadvantages include: Less Range (<50) for controlling Devices, Pairing Process, and Requires Human Involvement for control. No Remote Control or Monitoring.

In [2] the author's implements home automation system using Arduino board that comes along with various sensors such as PIR motion sensor etc. and uses a GSM technology. The status of all the devices connected is sensed by the Arduino board for further processing. This system ensures home automation and security. Arduino board is an advanced version of microcontroller. It has various disadvantages similar to microcontrollers: Less Friendly Environment for development, Less Flexible, Maintenance Overhead.

In [3] the author's has proposed a home automation system using Arduino board based on IOT domain. This particular system uses an internet protocol-based communication. This system makes use of three operating modes: manual mode, automated mode and security mode. The manual mode is based on web supporting device, automated mode is based on sensor reading and security mode is based on safety. The simple execution is provided by Arduino microcontrollers that are used in this project as compared to other controllers. This particular prototype also uses Wi-Fi routers. The shortcomings are: Less Friendly Environment for development, Less Flexible, Maintenance Overhead.

In [4] the author presents the implementation of WIFI based home automation system. Wi-Fi technology is used for connecting various parts of the infrastructure. The proposed system includes a server where the status of each connected device is updated anytime it changes so that the user or system administrator can remotely control as well as monitor the system. It also includes hardware interface modules for connecting various sensors and actuators. This system provides power management and security. The disadvantages are: since WIFI usage involves a range, it is not possible for remote monitoring. It is not much reliable since the WIFI may go down at any point of time.

In [5] the author has designed a PIC microcontroller using ZigBee technology. The home appliances are controlled by using two technologies namely GSM network technology and speech recognition. In case smokeis detected in the house the SMS is sent to the mobile by using a GSM modem which is connected to the PIC controller. The ZigBee and GSM technologies are used for wireless communication among various modules. The microcontroller senses the accidents. It has disadvantages such as: use of Microcontroller – Requires Burning of Code for every Changes, Interface Problems, Maintenance overheads, Low processing power, Less Flexible due to complex architecture.

3. PROJECT DESCRIPTION

Block diagram

In our project totally we have 4 main blocks those are

1) Power supply
2) ESP 32
3) Smoke Sensor
4) Finger Sensor
5) ESP32 Cam
6) GSM module

Technology and Software Details

1) The IOT technology is used to controlled the home devices through website
2) The Security for door locking system is through finger recognition technology
3) The Sensors like smoke sensors , fire sensor, etc. is used for automation for the home safety
4) The GSM Technology is used for SMS for controlling the devices as well as for alerting the concerning the peoples by calling.

The Internet of Things (IoT) refers to a network of physical objects that are embedded with sensors, software, and other technologies to enable them to connect and exchange data with other devices and systems over the internet or other networks. The primary function of an IoT system is to collect and exchange data in real-time. Typically, an IoT system comprises of three main components:

Smart devices: These are physical objects such as smart thermostats, security cameras, or fitness trackers that are equipped with computing capabilities. They gather data from their surroundings, user inputs, or usage patterns, and then transmit this data over the internet to an IoT application.

IoT application: An IoT application is a collection of software and services that aggregate data from multiple IoT devices. Machine learning or artificial intelligence (AI) technologies are often used to analyse this data to make informed decisions. These decisions are then communicated back to the IoT devices, which respond accordingly.

Graphical user interface (GUI): The IoT device or group of devices can be managed through a GUI. This may be in the form of a mobile application or website that enables users to register and control their smart devices. The GUI also allows users to monitor and manage the data generated by their IoT devices

Software Details

1) Android Studio is used for developing application for the security system
2) PHP language is used for developing the website for the system
3) ARDUINO IDE compiler is used and programmed with C++ for developing the firmware for the hardware system

Android Studio is the official Integrated Development Environment (IDE) for android application development. Android Studio provides more features that enhance our productivity while building Android apps.

Android Studio was announced on 16th May 2013 at the Google I/O conference as an official IDE for Android app development. It started its early access preview from version 0.1 in May 2013. The first stable built version was released in December 2014, starts from version 1.0.

Since 7th May 2019, Kotlin is Google's preferred language for Android application development. Besides this, other programming languages are supported by Android Studio.

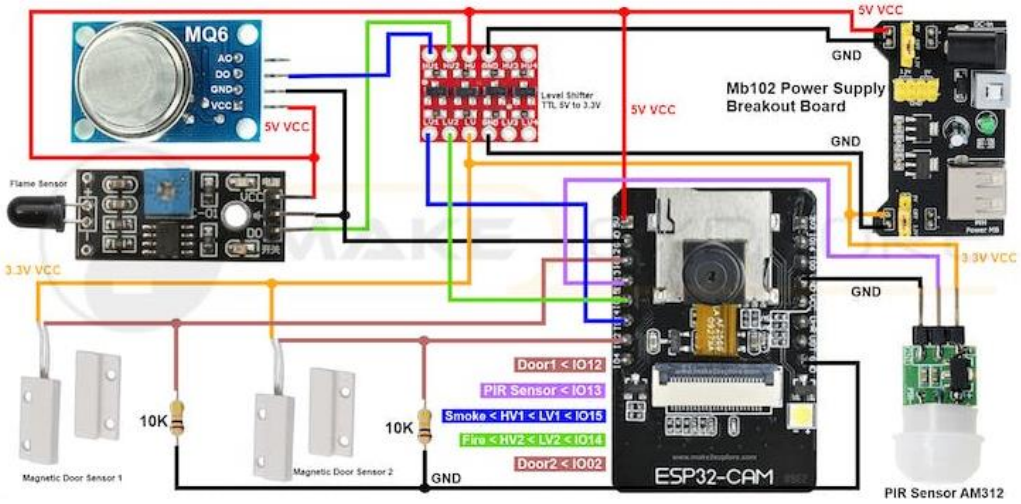
Features of Android Studio

- It has a flexible Gradle-based build system.
- It has a fast and feature-rich emulator for app testing.
- Android Studio has a consolidated environment where we can develop for all Android devices.
- Apply changes to the resource code of our running app without restarting the app.
- Android Studio provides extensive testing tools and frameworks.
- It supports C++ and NDK.
- It provides build-in supports for Google Cloud Platform. It makes it easy to integrate Google Cloud Messaging and App Engine.

PHP Language.

PHP (recursive acronym for `PHP: Hypertext Preprocessor`) is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML.

Circuit Diagram



Software

Step 1 - Installing Boards and Tools

We'll program the ESP32-CAM board using Arduino IDE, so make sure you have it installed in your Arduino IDE. You can check out following video for that, there we have explained in detail about how to install ESP boards into an Arduino IDE

Step 2 - Installing libraries

For this project you need to install several libraries.

==> Android Studio Bot Library, ArduinoJson Library

The following library can be installed through the Arduino Library Manager. Go to **Sketch** > **Include Library**> **Manage Libraries** and search for the library name.

- ArduinoJson Library : you have to install the ArduinoJson library

==> Universal Android Bot Library

To interact with the Android bot, we'll use the Universal Android Studio Bot Library created by Brian Lough that provides an easy interface for the Android Bot API.

Follow the next steps to install the latest release of the library.

- Go to Arduino IDE, **Sketch > Include Library > Add.ZIP Library...**
- Add the library you've just downloaded.

Important Note: don't install the library through the Arduino Library Manager because it might get install a deprecated version.

Step 3 - Code of the project is given below, with libraries. It is also available on our GitHub. We have explained code in following video, check out to learn more

Step 4 - In software setup, You need to complete following four steps

1. We need Android Studio Application to be Installed on our smartphone.

2. Get Your Android Studio Chat ID -

- Why ? - To chat with an Authorized User ESPCAM needs USER ID / CHAT ID of our Android Studio
- Because anyone that knows your bot username can interact with it. To make sure that we ignore such spam messages that are not from our Android Studio account (or any authorized users). We need to get our Android Studio Chat ID.
- Whenever your Android Studio bot receives a message, the ESP CAM Board can check whether the sender ID corresponds to your User ID and if it is correct then and then only it handle the message.

3. Create Android Studio Bot -

- Create Android Studio bot for our Home Security Application/Project
- Chat with Masterbot named "*BotFather*" to create a new bot

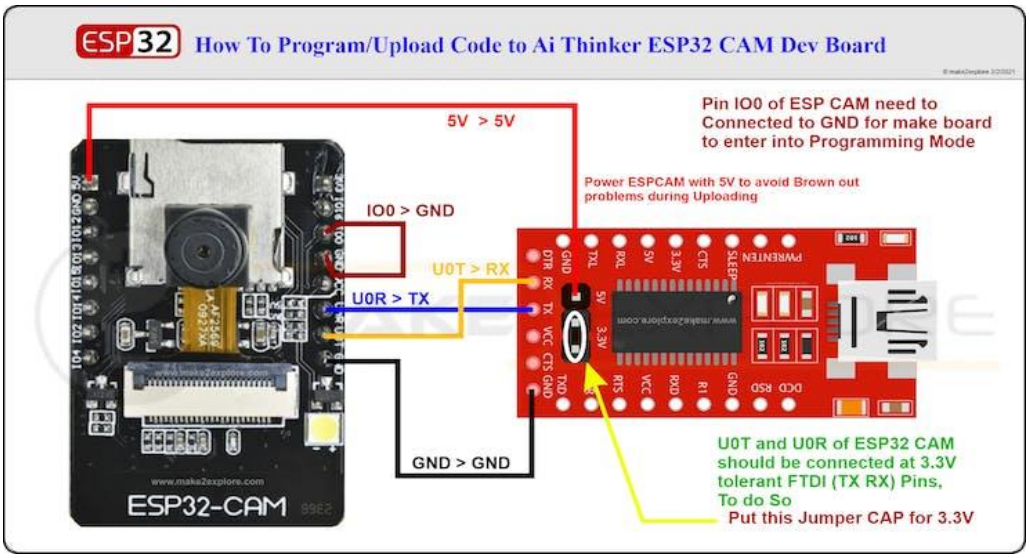
4. Get Bot Token -

- When you create new bot – "*BotFather*" will issue a new bot token for your bot
- Save the bot token because you'll need it later (to Enter it in code) so that the ESP32 CAM can interact with the bot.

So we've explained all above steps in following video, check out and complete all above steps

Step 5 - Programming ESP32-CAM Dev Board - to program the ESP32-CAM you need to setup following

circuitry



You can Check out following video, where we have explained How to program ESP32-CAM Dev Board

ARDUINO IDE

The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them.

Writing Sketches
Programs written using Arduino Software (IDE) are called **sketches**. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom righthand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor.

Hardware Used

ESP32 CAM

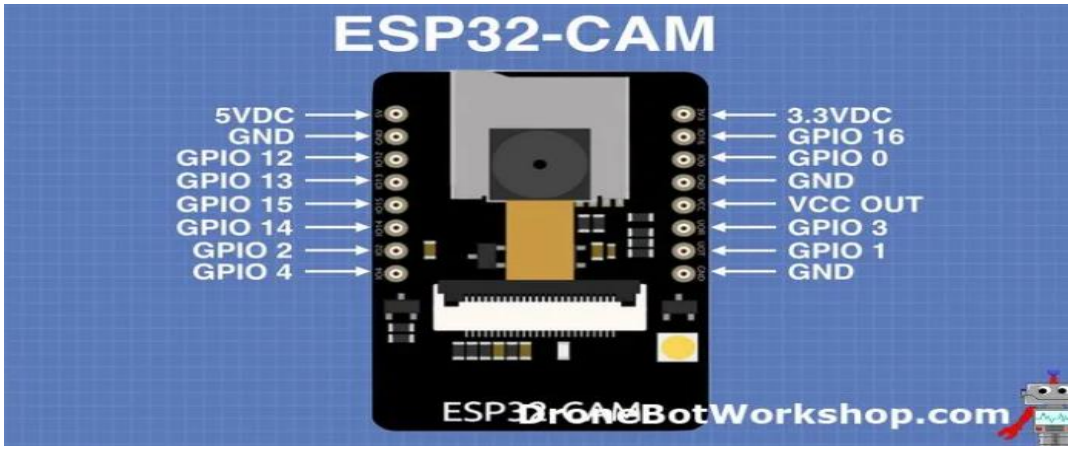
The ESP32 CAM WiFi Module Bluetooth with OV2640 Camera Module 2MP For Face Recognization has a very competitive small-size camera module that can operate independently as a minimum system with a footprint of only 40 x 27 mm; a deep sleep current of up to 6mA and is widely used in various IoT applications.

It is suitable for home smart devices, industrial wireless control, wireless monitoring, and other IoT applications.

This module adopts a DIP package and can be directly inserted into the backplane to realize rapid production of products, providing customers with high-reliability connection mode, which is convenient for application in various IoT hardware terminals.

ESP integrates WiFi, traditional Bluetooth, and BLE Beacon, with 2 high-performance 32-bit LX6 CPUs, 7-stage pipeline architecture. It has the main frequency adjustment range of 80MHz to 240MHz, on-chip sensor, Hall sensor, temperature sensor, etc.

Pin Diagram



Features:

ESP32-CAM:

1. The smallest 802.11b/g/n Wi-Fi BT SoC module.
2. Low power 32-bit CPU, can also serve the application processor.
3. Up to 160MHz clock speed, summary computing power up to 600 DMIPS.
4. Built-in 520 KB SRAM, external 4MPSRAM.
5. Supports UART/SPI/I2C/PWM/ADC/DAC.
6. Support OV2640 and OV7670 cameras, built-in flash lamp.

7. Support image WiFI upload.
8. Supports TF card.
9. Supports multiple sleep modes.
10. Embedded Lwip and FreeRTOS.
11. Supports STA/AP/STA+AP operation mode.
12. Support Smart Config/AirKiss technology.
13. Support for serial port local and remote firmware upgrades (FOTA).

Specifications:

1. Wireless Module: ESP32-S WiFi 802.11 b/g/n + Bluetooth 4.2 LE module with PCB antenna, u.FL connector, 32Mbit SPI flash, 4MBit PSRAM.
2. External Storage: micro SD card slot up to 4GB.
3. Camera
    - FPC connector.
    - Support for OV2640 (sold with a board) or OV7670 cameras.
    - Image Format: JPEG(OV2640 support only), BMP, grayscale.
    - LED flashlight.
4. Expansion: 16x through-holes with UART, SPI, I2C, PWM.
5. Misc: Reset button.
6. Power Supply: 5V via pin header.
7. Power Consumption.
    - Flash LED off: 180mA @ 5V.
    - Flash LED on to maximum brightness: 310mA @ 5V.
    - Deep-sleep: 6mA @ 5V min.
    - Modem-sleep: 20mA @ 5V min.
    - Light-sleep: 6.7mA @ 5V min.
8. Dimensions (ESP32): 40 x 27 x 12 (LxWxH) mm.
9. Temperature Range: Operating: -20 ℃ ~ 85 ℃; storage: -40 ℃ ~ 90 ℃ @ < 90%RH.

Research Methodology

1) This Devices Control through Internet of Things (IOT) Methodology

2) The Zero Crossing Method used to Control the AC energy through PWM (Pulse Width Modulation)

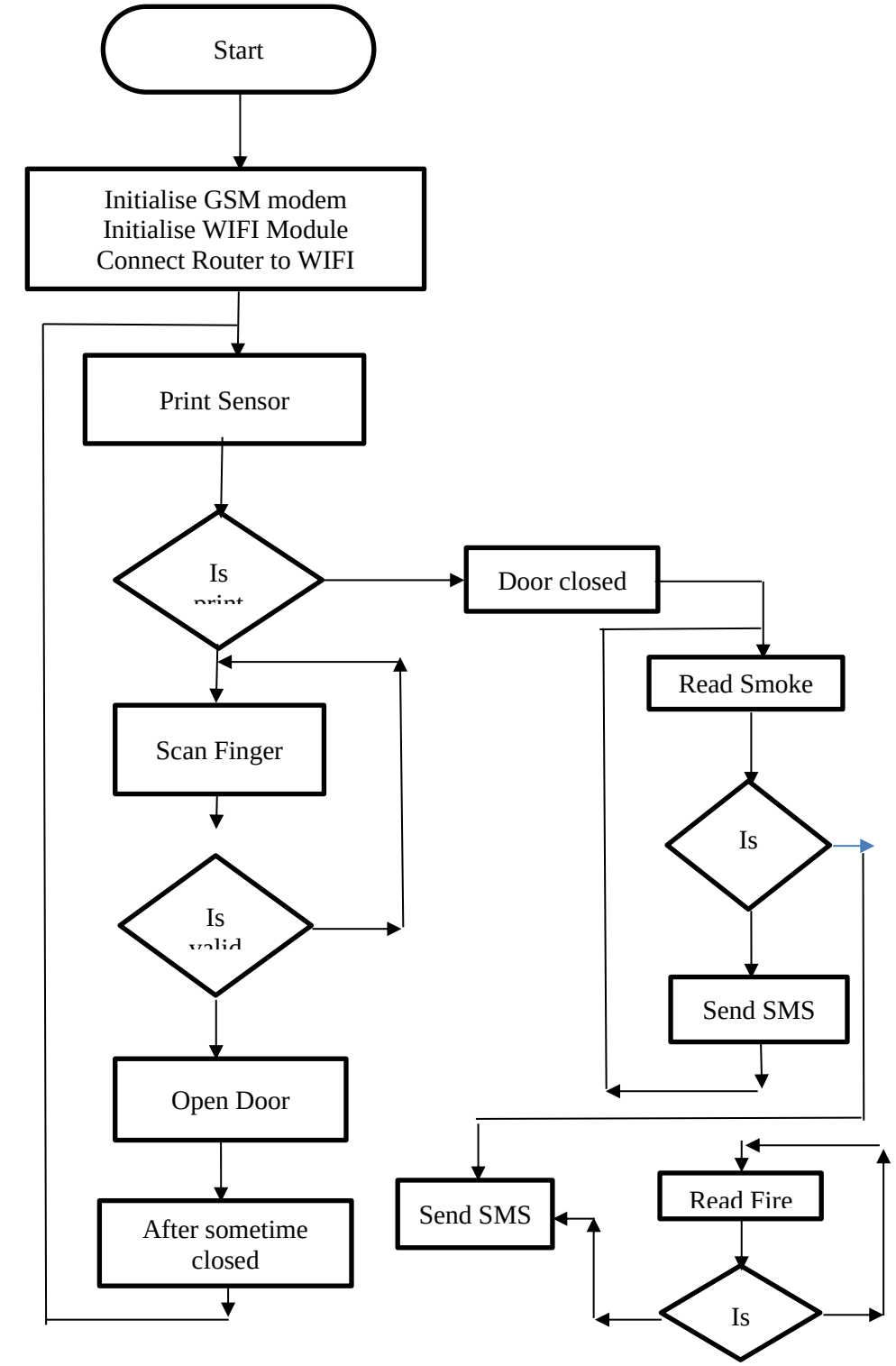
3) The WI-FI device used to communicate with the electrical equipment and to control it.

4) The IP address method is used to communicate through Client Server methodology.

5) The System will Manually as well as wireless based

6) Android application through Software based methodology

Flow of the System



The project have multiple modules likes , smoke detection, finger printer based door locking system, video streaming, electric home appliances controls through website and mobile. The IOT technology is used to integrate the all modules. The WIFI Module is used to control the devices and security devices. The WIFI module will be connected with WIFI router. The data will be sending to the server or the client will accept the data from the server. The electric devices will be control through website. The buttons likes kitchen room devices, living room devices, etc. will be on the website. This button be used to control the electric devices online.

ADVANTAGES

1) The home automation and security system will maintain home safety.
2) Contactless switches will have safety for human beings
3) The System can be used by anyone. No training is required for this.
4) The System will be cost effective
5) It will safe home from intruders or from thefts

References

1. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys and Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourth Quarter 2015.
2. R. Bhatt, S. Saini, and S. S. Saini, "Internet of Things: Architectures, Protocols, and Applications," Journal of Microelectronics, Electronic Components and Materials, vol. 47, no. 2, pp. 79-89, 2017.
3. S. Nourizadeh and N. Moghadam, "Internet of Things: A Review on Technologies, Protocols, and Applications," International Journal of Computer Science and Information Security, vol. 15, no. 4, pp. 167-179, 2017.
4.A. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, September 2013.
5. M. U. Khan, M. N. Ullah, and S. A. Madani, "Internet of Things (IoT): Architecture and Challenges," in 2014 International Conference on Future Internet of Things and Cloud, 2014, pp. 15-20.
6. Y. Yan, H. Zhang, and S. K. Das, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, October 2017.
7. S. H. Khan, S. A. Madani, M. U. Khan, and A. Zomaya, "Internet of Things (IoT): Applications, Challenges, and Opportunities," in 2012 International Conference on Advanced Computer Science Applications and Technologies, 2012, pp. 224-229.
8. K. Lee, K. Lee, and J. Kim, "Smart Home Automation: A Literature Review," Journal of Security Engineering, vol. 14, no. 3, pp. 227-233, 2017.