IoT Based Home Automation and Security System with Intruder Recognition Feature

***Abstract*—In the era of technological revolution, life is becoming easier as automation affects all aspects of life. Human life is becoming more secure, comfortable, and efficient. By implementing technologies and devices like the Internet of Things(IoT), and sensors in home systems, it is possible to stratify the home system making fire and gas detection simpler, and also protect the home from intruders. Even if any anomaly occurs, the user can know about it. Both hardware and software work in harmony to create a seamless and personalized living experience. Smart home enables remote access and control of devices through smartphones or voice commands, allowing users to adjust settings, monitor activities, and receive alerts from anywhere. They enhance safety and security through real-time surveillance, intrusion detection, and smart locks, providing peace of mind to homeowners even when they are not at home. However there is a concern regarding privacy breach, but that is possible to overcome. Regarding all factors, smart homes represent a paradigm shift in residential living, offering unparalleled convenience, efficiency, and safety. While they hold tremendous promise for enhancing our quality of life, addressing privacy, security, and usability concerns is imperative to realize their full potential. In this work, we propose a smart home automation system with enhanced fire and gas detection, improved security, and an advanced intruder recognition feature.**

***Index Terms*—Blynk, Sensors, ESP32, IoT, Base64**

I. Introduction

The idea of smart houses has changed due to the Internet of Things (IoT), which gives homeowners more efficiency, security, and control [1]. As the demand for automation and remote access grows, smart home solutions need to be able to combine several functions into one intuitive platform. The goal of this work is to create an Internet of Things (IoT)–based smart home system that increases security, maximizes resource utilization, and improves convenience. The goal is to provide a complete solution that takes into account different facets of home automation by utilizing contemporary technologies.

Automating vital safety features like gas and fire detection while integrating more conventional security measures like password protection and alarm systems are the core features of this proposed prototype. Even while some of these characteristics was present in earlier systems separately, they were not integrated into a single framework. By combining these components into a single ”super module,” this method guarantees a smooth and effective security system that the homeowner can readily monitor and control.

The ESP32 microcontroller, which has strong processing capabilities and Wi-Fi connectivity for real-time monitoring, was used to create this system. Furthermore, the integration of the Blynk IoT platform enabled consumers to remotely monitor and control their home security system via a smartphone application. This combination improves convenience and security by allowing homeowners to remain connected to their houses at all times, even when they are away.

This system seeks to maximize resource use in the house in addition to security. It helps cut down on wasteful power use and improves the energy efficiency of the house by automating several tasks, including environmental monitoring and energy management. These features provide homeowners complete control over how their home is run while also making living spaces smarter and more sustainable.

In conclusion, this system provides a password-based protection system with a security camera feature that captures intruder's images and stores them. Fire and Gas sensors are installed with a central MUX system to detect any abnormality and with the help of Blynk and ESP32, any hazardous incident will trigger notification to the user. In brief, our proposed system has the following features:

- Automated fire and gas detection
- Encrypted password-protection
- Intruder image capturing feature
- Real-time data sent to the owner in case of any problem
- Custom multiplexing circuit to include scalability

II. Related Works

The Internet of Things (IoT) has transformed smart home systems by integrating automation, and remote control to enhance safety, convenience, and efficiency. Many recent works have focused on improving security, energy management, and communication protocols, yet challenges remain in scalability, interoperability, and data privacy.

In the proposed methodology by Cristina et al. [2]., a system for interconnecting sensors, actuators, and other data sources with the purpose of multiple home automation was suggested. Their solution is cost-effective, small, and easy to work with. Kang et al. [3] used embedded system, 3G, and ZIGBEE technologies to overcome the drawbacks of current smart home systems such as discrete functions, poor portability, weak updating capability, and personal computer dependence. Moreover, the system architecture was also presented, and the design of its gateway was shown in detail from hardware to software in their work.

Geneiatakis et al. [4] discussed various issues for an IoT-based smart home. Li et al. [5] revolved their work against the smart home-to-grid system. They introduced a UEP as an indicator of differential pricing in dynamic domestic electricity

tariffs. Their system can automatically schedule the operation of home appliances.

The proposed prototype by Gupta et al. [6] mainly concentrates on power and security management. They implemented an Ethernet-based Smart Home intelligent system for monitoring the electrical energy consumption based upon the real-time tracking of the devices at home an INTEL GALILEO 2ND generation development board.

Hoque et al. [7] suggested an architecture for a cost-effective smart door sensor that will inform a user through an Android application, of door open events in a house or office environment. Another notable work by Singh et al. [8] implemented a sensor node for home automation.

A. Motivation:

While numerous studies have focused on security systems, they often lack the flexibility for users to modify passwords at will and the inclusion of an intruder alert mechanism. Moreover, relying solely on a password is insufficient, as systems remain vulnerable to hacking. To enhance security, encryption of passwords is essential—an aspect that recent works have largely overlooked.

III. Implementation Details

In this study, we have developed a next-generation highly modular home-security system using esp-32 and a custom multiplexer circuit that enables the user to modify the system according to their need. Our system can perform fire and smoke detection and alert the user of any such incident through the custom Blynk Android interface. The system also integrates an intelligent door-lock mechanism which can be only accessed through an encrypted password system. In case a potential intruder tries to hack in using brute force, the onboard esp32-camera would get activated and send a picture of the potential intruder to the owner's Google account.

The blynk api serves as the main back-end which logs in all the sensor data to its user account. The overall system architecture is given in Fig. 1.

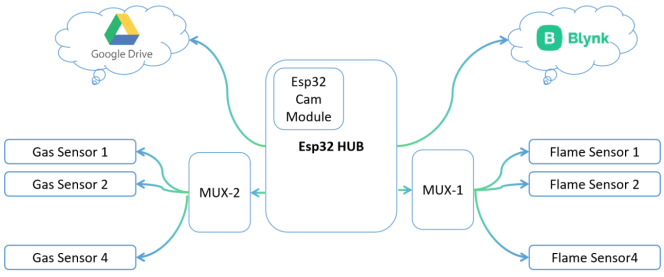

Fig. 1. System Architecture.

A. ESP-32 Hub

In our project, the ESP-32 serves as the central hub for system control and communication. It is responsible for hosting the main binary code that orchestrates the entire system's operation, ensuring seamless coordination between the various components. Additionally, the ESP-32 runs the Blynk Edgent client, which establishes a connection with the Blynk server to facilitate real-time monitoring and the publication of sensor data. The system also incorporates a secure password management feature, where the ESP-32 stores a hashed 6-digit PIN code provided by the user, ensuring secure access control. Furthermore, the ESP-32 manages the operation of the ESP32-CAM module, sending signals via a digital pin to trigger its capture and transmission subroutine in response to potential intrusion events. This integration of multiple functionalities within a single ESP-32 platform enhances the system's efficiency, security, and adaptability.

B. Clock Generation

A multi-vibrator was used in astable mode to generate a clock of a desired frequency. Then the knowledge of logic circuits such as a counter was used to generate a frequency half of the clock. These two clocks were used as the control signal bits of the MUX. Buck Module is used for a regulated power supply. A CD4047 multivibrator was used in astable mode to generate a clock signal of the desired frequency. This clock serves as the primary timing source for the multiplexer operation to generate a control signal with half the frequency of the original clock, an IC74HC191 counter was employed. This counter divides the clock frequency by two and produces the Most Significant Bit (MSB) of the control signal required by the MUXs.The process for our custom clock generator circuit is given in Fig. 2.

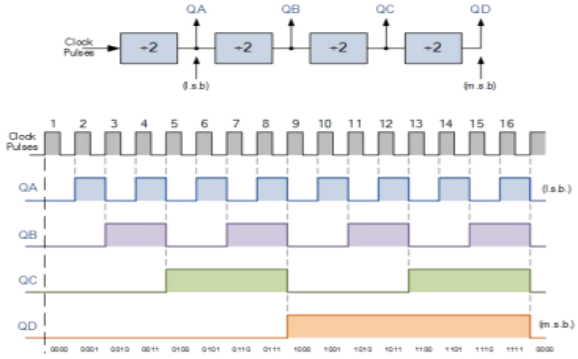

Fig. 2. Frequency Division by Counter

C. Custom MUX circuit

In order to effectively cycle through all available sensor nodes and register their values, we developed a custom multiplexer (MUX) circuit. This design enables the sequential selection of sensor nodes using a controlled clock signal.

The schematic diagram for our custom multiplexer circuit is given in Fig. 3.

D. PCB Design

We designed and fabricated a custom Printed Circuit Board (PCB) to seamlessly integrate it into our primary system

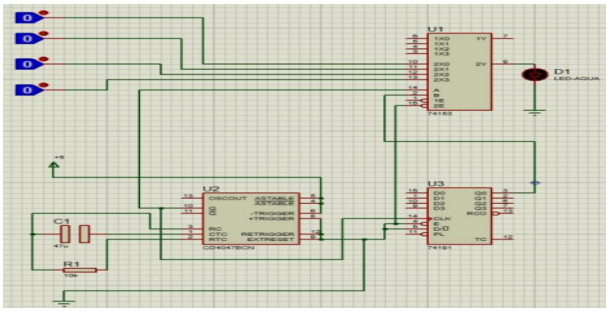

Fig. 3. Schematics of our custom multiplexer circuit.

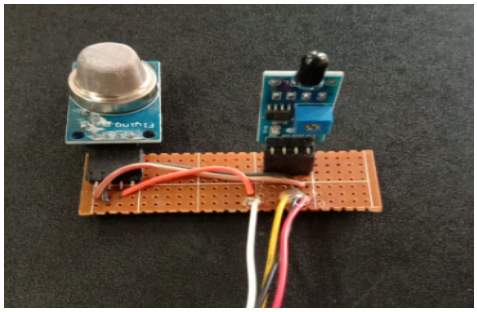

Fig. 5. Modular Sensor Nodes.

architecture. This PCB serves as a crucial interface, facilitating efficient data acquisition and communication between various sensing elements and the central processing unit. To ensure modularity and ease of deployment, the PCB is equipped with multiple sensor ports, which act as insertion points for our modular sensor nodes. This PCB layout is designed only in one layer which is very cost-effective and simple to build, adding to the scalability and affordability of the design. The PCB layout was meticulously designed using Proteus, incorporating industry best practices to optimize signal integrity, minimize noise, and enhance overall system reliability. The finalized layout, as illustrated in Fig. 4, underwent rigorous validation to ensure compliance with electrical and mechanical design constraints, thereby enabling seamless integration into the overall system architecture.

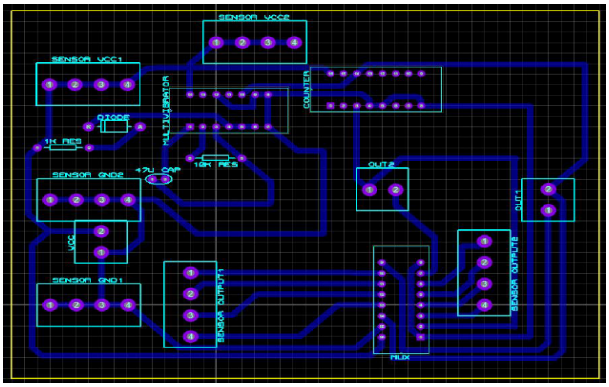

Fig. 4. PCB Layout in Proteus

E. Modular Sensor Nodes

Our fire detection circuits act as modular nodes that are connected to the ESP-32 HUB through the custom MUX circuit. Each node consists of two sensors. For Fire detection, the sensor that we used is Flame Sensor(KY-026 Series) which is connected to the inputs of MUX-1, and for smoke detection, we used the MQ-9 series smoke detector which is connected to the inputs of MUX-2. The custom circuit is given in Fig.3. Ensures that all the data generated from available sensors are accessed sequentially. The physical construction of these sensor nodes is given in Fig. 5.

F. Password Protection & Modification System

One of the core features of our proposed smart home prototype is a password-protected entrance, along with providing the user the scope to modify passwords at will. The password will be typed through a 4*4 membrane keyboard. The overall password protection system algorithm is explained in detail in Algorithm 1. The password length is fixed to 6 digits to simplify the overall system.

Algorithm 1 Secure Password Authentication and Modification

Input: User enters a 6-digit password
if User enters '#' **then**
    Compare input password with stored password in EPROM
    if Password matches **then**
        Open the door
    else
        Prompt user to retry password entry
        if Second attempt is incorrect **then**
            Capture user's image
        end if
    end if
else if User enters '*' **then**
    Enter password modification mode
    Compare input password with stored password in EPROM
    if Password matches **then**
        Allow user to enter a new password
        Save the new password to EPROM (erasing the previous one)
    else
        Prompt user to retry password entry
        if Second attempt is incorrect **then**
            Capture user's image
        end if
    end if
else
    Reset password entry process and allow the user to re-enter the password
end if

The captured image is then sent to the homeowner.

G. Vision-based Intruder alert System

In the event of a brute-force attack on the authentication system, an intrusion detection mechanism is triggered to capture an image of the unauthorized user. This system is implemented using an ESP32-CAM module, which operates autonomously and is programmed to upload the captured images to cloud storage via the Google Drive API. The ESP32-CAM continuously monitors access attempts and seamlessly integrates with the security framework to enhance threat mitigation.

Google Drive API does not support direct uploading of binary image data via HTTP POST. Therefore, the image is first encoded into a Base64 string, which allows it to be transmitted as text within an HTTP request payload. The flow of the process is given in Fig 6.

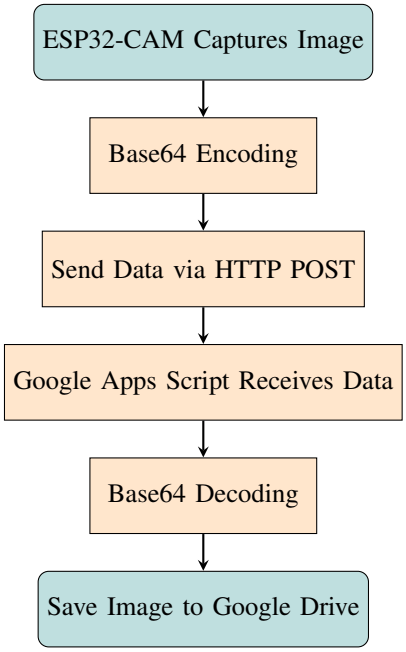

Fig. 6. Flowchart of ESP32-CAM Image Capture and Upload Process

The ESP32-CAM captures an image and encodes it into Base64 format using an optimized encoding algorithm. The encoding process involves converting raw binary image data into ASCII characters using a lookup table and bitwise operations, ensuring compatibility with text-based transmission protocols.

A Google Apps Script (GAS) endpoint processes the received Base64-encoded image, decodes it back into binary format, and saves it in Google Drive. The script organizes files into date-based hierarchical folders, automatically creating subdirectories as needed. The ESP32-CAM communicates via HTTP POST requests, transmitting image data efficiently. The entire process ensures secure, structured, and automated cloud storage for captured images, enabling remote monitoring.

H. Hardware Overview

We have successfully developed the hardware for our system, which is divided into two distinct units: the Outdoor Unit (ODU) and the Indoor Unit (IDU). Fig. **??** The ODU is primarily responsible for capturing images of potential intruders' faces and recording user password input via the keypad. It integrates the ESP32-CAM module, which serves as a vital component for visual monitoring and surveillance, along with a keypad for entering user credentials as shown in Fig. **??**. This combination allows for the real-time capture of images or video footage, which can be used for detecting potential intrusions or for documenting specific events. The ODU is designed to be deployed in outdoor environments, where it can effectively monitor external conditions while being seamlessly connected to the Indoor Unit.

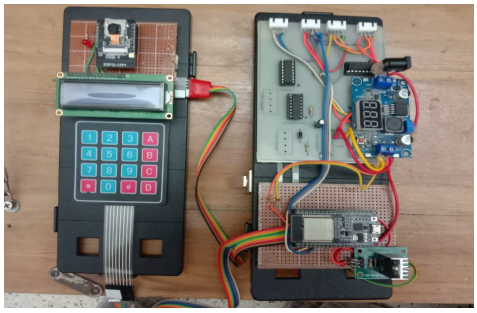

Fig. 7. Hardware Overview ,Outdoor-unit(Left) and Indoor-unit(Right.

The IDU, on the other hand, functions as the central control unit of the system. It houses the ESP32 hub, which coordinates the overall operation and communication between the various sensors and peripherals. The IDU includes multiple sensor ports to facilitate the connection of various modular sensors, allowing for flexible expansion and adaptability to different sensing requirements. Additionally, the Indoor Unit manages the processing, storage, and transmission of the data collected by the sensors and ODU, ensuring smooth operation and real-time feedback. Together, these two units form a comprehensive system that provides both remote surveillance and local control, ensuring a robust and efficient solution for monitoring and interaction.

I. Blynk User-Interface

For real-time fire detection and user notification, we have developed a web-based and mobile-accessible user interface (UI) integrated with the Blynk IoT platform. The UI, illustrated in Fig. 8, can be accessed via a dedicated Blynk client application or through any web browser, enabling seamless remote monitoring. The system is configured to trigger automated push notifications upon detecting fire or smoke, ensuring prompt alerts. This notification mechanism is implemented using event-driven programming, leveraging sensor data processing and cloud-based communication protocols for reliable and low-latency alerts.

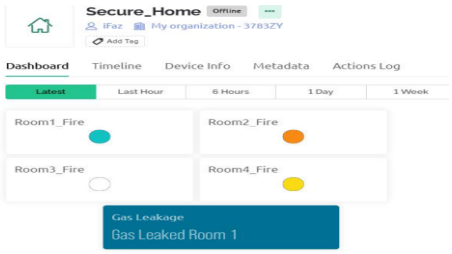

Fig. 8. User Interface(UI).

Our system leverages Over-The-Air (OTA) updates using Blynk. Edgent to enable seamless user credential provisioning without requiring direct access to the device's binary code. This dynamic provisioning mechanism allows users to configure Wi-Fi credentials and authentication tokens remotely during the initial setup. Through Blynk.Edgent's built-in Wi-Fi manager, the IoT module enters provisioning mode on first boot, allowing users to input their credentials via the Blynk mobile app or a captive portal. This eliminates the need for manual firmware modification, streamlining deployment while maintaining security and ease of use.

IV. Testing and Results

Our tests suggest that the sensitivity of this sensor depends somewhat on ambient lighting. Initially, we calibrated each sensor so that we could detect small lighter fires from a close distance for the sake of our project demonstration. For gas leakage detection we used an MQ-9 Gas sensor. During our market research, we came across several types of gas sensors

Sensor Name	Gas to Measure
MQ-2	Methane, Butane, LPG, Smoke
MQ-3	Alcohol, Ethanol, Smoke
MQ-4	Methane, CNG Gas
MQ-5	Natural gas, LPG
MQ-7	Carbon Monoxide
MQ-8	Hydrogen Gas
MQ-9	Carbon Monoxide, Flammable gases
MQ131	Ozone

TABLE I
Gas Sensors and Their Measured Gases

Our system deals with a house hold monitoring system, hence detection of flambe gas was our priority. Our findings suggests that MQ-9 series is best suited for this application.

V. Conclusion

This project effectively illustrates a dependable and effective Internet of Things (IoT)-based smart home system that combines several automation and security elements into a single framework. Combining alarm systems, password protection, and gas and fire detection guarantees complete home security while maximizing resource utilization. The solution improves convenience and safety by enabling remote access and real-time monitoring through the use of the Blynk IoT platform and the ESP32 microcontroller. The outcomes validate its efficacy, offering homes a reliable option that reacts quickly to possible dangers. This study provides a solid basis for upcoming developments in smart home technology because of its scalability, affordability, and user-friendliness, guaranteeing that contemporary homes stay safe, connected, and energy-efficient.

References

[1] Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." Journal of cleaner production 140 (2017): 1454-1464.
[2] Stolojescu-Crisan, Cristina, Calin Crisan, and Bogdan-Petru Butunoi. "An IoT-based smart home automation system." Sensors 21.11 (2021): 3784.
[3] Bing, Kang, et al. "Design of an Internet of Things-based smart home system." 2011 2nd International Conference on Intelligent Control and Information Processing. Vol. 2. IEEE, 2011.
[4] Geneiatakis, Dimitris, et al. "Security and privacy issues for an IoT based smart home." 2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO). IEEE, 2017.
[5] Li, Xiao Hui, and Seung Ho Hong. "User-expected price-based demand response algorithm for a home-to-grid system." Energy 64 (2014): 437-449.
[6] Gupta, Punit, and Jasmeet Chhabra. "IoT based Smart Home design using power and security management." 2016 international conference on innovation and challenges in cyber security (iciccs-inbush). IEEE, 2016.
[7] Hoque, Mohammad Asadul, and Chad Davidson. "Design and implementation of an IoT-based smart home security system." International Journal of Networked and Distributed Computing 7.2 (2019): 85-92.
[8] Singh, Himanshu, et al. "IoT based smart home automation system using sensor node." 2018 4th International Conference on Recent Advances in Information Technology (RAIT). IEEE, 2018.