Mini Project Patent Document

On

Smart Security Platform for Resource constraint IOT

Submitted to the

Department of Computer Science & Engineering – IoT

In partial fulfilment of the requirements

For the degree of

BACHELOR OF TECHNOLOGY

Submitted to:- Dr. Gambhir Singh

Submitted By

Priyam Kumar	Roll. No. 2201321550041
Nikhil Sagar	Roll. No. 2201321550036
Prince Raj	Roll. No. 2201321550040
Parmanand Singh	Roll. No.2201321550039

Greater Noida Institute of Technology (Engg. Institute), Greater Noida

Dr. A.P.J. Abdul Kalam Technical University, Lucknow

February, 2024

ABSTRACT

Introduces a cutting-edge home security system leveraging Internet of Things (IoT) technology with Passive Infrared (PIR) sensors and microcontrollers, seamlessly integrated with the widely used messaging platform, WhatsApp. The central component of the system is a microcontroller, orchestrating the collaboration between PIR sensors strategically placed in key areas and the WhatsApp API for real-time communication.

The PIR sensors continuously monitor the designated areas for motion, promptly signaling the microcontroller upon detection. The microcontroller, in turn, activates a camera module to capture images or short video clips of the detected motion. Integrating with the WhatsApp API enables the system to deliver instant notifications to homeowners, including visual data captured during the event.

Customization features allow users to define specific detection zones, adjust sensitivity levels, and tailor notification preferences through the microcontroller. The system supports multiple users, facilitating collaborative monitoring and ensuring a collective approach to home security.

This IoT-based home security solution combines the efficiency of PIR sensors, the processing capabilities of microcontrollers, and the ubiquitous communication medium of WhatsApp. The seamless integration of these technologies enhances the responsiveness and accessibility of the system, providing homeowners wit

BACKGROUND OF THE PROJECT

1. **Need for Smart Security Solutions**: With the advancement of technology and the increasing demand for smart home and business solutions, there has been a growing need for smarter and more connected security systems.
2. **ESP32 Microcontroller**: The ESP32 microcontroller, developed by Espressif Systems, offers a powerful platform with integrated Wi-Fi and Bluetooth capabilities, making it ideal for IoT applications. Its low-cost, low-power features make it suitable for a wide range of projects.
3. **Integration of Sensors and Actuators**: In the ESP32 security system, various sensors such as motion detectors, door/window sensors, temperature sensors, and cameras can be integrated with the microcontroller. These sensors detect changes in the environment and trigger actions based on predefined conditions.
4. **Remote Monitoring and Control**: The ESP32 microcontroller can connect to the internet through Wi-Fi, allowing users to remotely monitor and control the security system using their smartphones, tablets, or computers. This remote access provides real-time notifications and alerts, enabling users to respond promptly to security events.
5. **Data Encryption and Security Protocols**: To ensure the security and integrity of data transmitted over the network, the ESP32 security system employs encryption protocols such as HTTPS and SSL/TLS. These protocols encrypt the communication between the microcontroller and the connected devices, preventing unauthorized access and tampering.
6. **Scalability and Customization**: One of the key advantages of the ESP32 security system is its scalability and customization options. Users can add or remove sensors, integrate third-party devices, and customize the system according to their specific security requirements.
7. **Energy Efficiency and Reliability**: The ESP32 microcontroller is designed for low-power operation, making it energy-efficient and reliable for continuous operation. It can be powered by batteries or connected to a power source, providing flexibility in deployment options.

Problems Addressed:

1. **Limited Connectivity**: Traditional security systems often rely on wired connections or proprietary protocols, limiting their flexibility and scalability. The ESP32 security system leverages Wi-Fi and Bluetooth connectivity, enabling wireless communication and remote monitoring capabilities.
2. **High Cost**: Conventional security systems can be expensive to install and maintain, especially for large properties or commercial buildings. The ESP32 microcontroller offers a cost-effective solution with its affordable hardware and open-source software platform.
3. **Complex Installation**: Installing traditional security systems typically requires professional expertise and extensive wiring, which can be time-consuming and labor-intensive. The ESP32 security system simplifies installation with its wireless connectivity and modular design, allowing users to easily set up and configure the system themselves.
4. **Limited Remote Access**: Traditional security systems often lack remote access features, making it difficult for users to monitor their property or respond to security events when they are away. The ESP32 security system provides remote access via

smartphones, tablets, or computers, allowing users to receive real-time notifications and control the system from anywhere with an internet connection.

5. **Lack of Integration**: Many traditional security systems operate as standalone solutions, making it challenging to integrate them with other smart home or IoT devices. The ESP32 security system supports seamless integration with a wide range of sensors, actuators, and third-party devices, enabling users to create custom automation routines and enhance their overall security posture.
6. **Security Vulnerabilities**: Traditional security systems may be susceptible to hacking, tampering, or signal interference, compromising the safety and privacy of the users. The ESP32 security system employs encryption protocols and security best practices to safeguard against unauthorized access and ensure the integrity of data transmitted over the network.

By addressing these challenges and providing a more accessible, affordable, and connected security solution, the ESP32 security system offers users greater peace of mind and enhanced protection for their homes, businesses, and asse

ADVATAGES OF THE PROJECT

1. **Wireless Connectivity**: The ESP32 controller supports Wi-Fi and Bluetooth connectivity, eliminating the need for extensive wiring and enabling flexible installation options. This wireless capability also facilitates remote monitoring and control of the security system from any internet-connected device.
2. **Low Cost**: The ESP32 microcontroller is a cost-effective solution for security system applications, offering powerful processing capabilities and integrated features at a relatively low price point. This affordability makes it accessible to a wide range of users, including homeowners, small businesses, and DIY enthusiasts.
3. **Open-Source Platform**: The ESP32 platform is based on open-source hardware and software, providing users with access to a wealth of resources, documentation, and community support. This openness fosters innovation and allows users to customize and extend the functionality of their security systems according to their specific requirements.
4. **Modularity and Scalability**: The ESP32 controller supports modular design principles, allowing users to easily expand and customize their security systems with additional sensors, actuators, and peripherals. This scalability enables users to tailor their systems to meet evolving security needs and accommodate changes in property size or layout.
5. **Integration with IoT Devices**: The ESP32 controller seamlessly integrates with a wide range of IoT devices and platforms, enabling users to create interconnected smart home ecosystems. By integrating their security systems with other IoT devices such as smart locks, cameras, and motion sensors, users can enhance the overall functionality and automation capabilities of their homes or businesses.
6. **Low Power Consumption**: The ESP32 microcontroller is designed for low power consumption, making it well-suited for battery-operated or energy-efficient applications. This feature is particularly useful for remote or off-grid installations where access to power sources may be limited.
7. **Security Features**: The ESP32 platform includes built-in security features such as encryption, secure boot, and secure storage, helping to protect against unauthorized access, tampering, and data breaches. These security measures enhance the overall integrity and reliability of the security system, ensuring the privacy and safety of users and their assets.

Overall, the ESP32 security system controller offers a compelling combination of affordability, flexibility, and functionality, making it an attractive choice for modern security applications. Its wireless connectivity, open-source platform, and integration capabilities enable users to create sophisticated and customized security solutions tailored to their specific needs and preferences.

SALIENT FEATURES OF THE PROJECT

Rich Peripheral Support: The ESP32 platform offers a wide range of built-in peripherals, including digital and analog interfaces, pulse-width modulation (PWM) outputs, I2C, SPI, and UART communication interfaces. These peripherals facilitate the integration of various sensors, actuators, and external devices, enabling versatile and customizable security system designs.

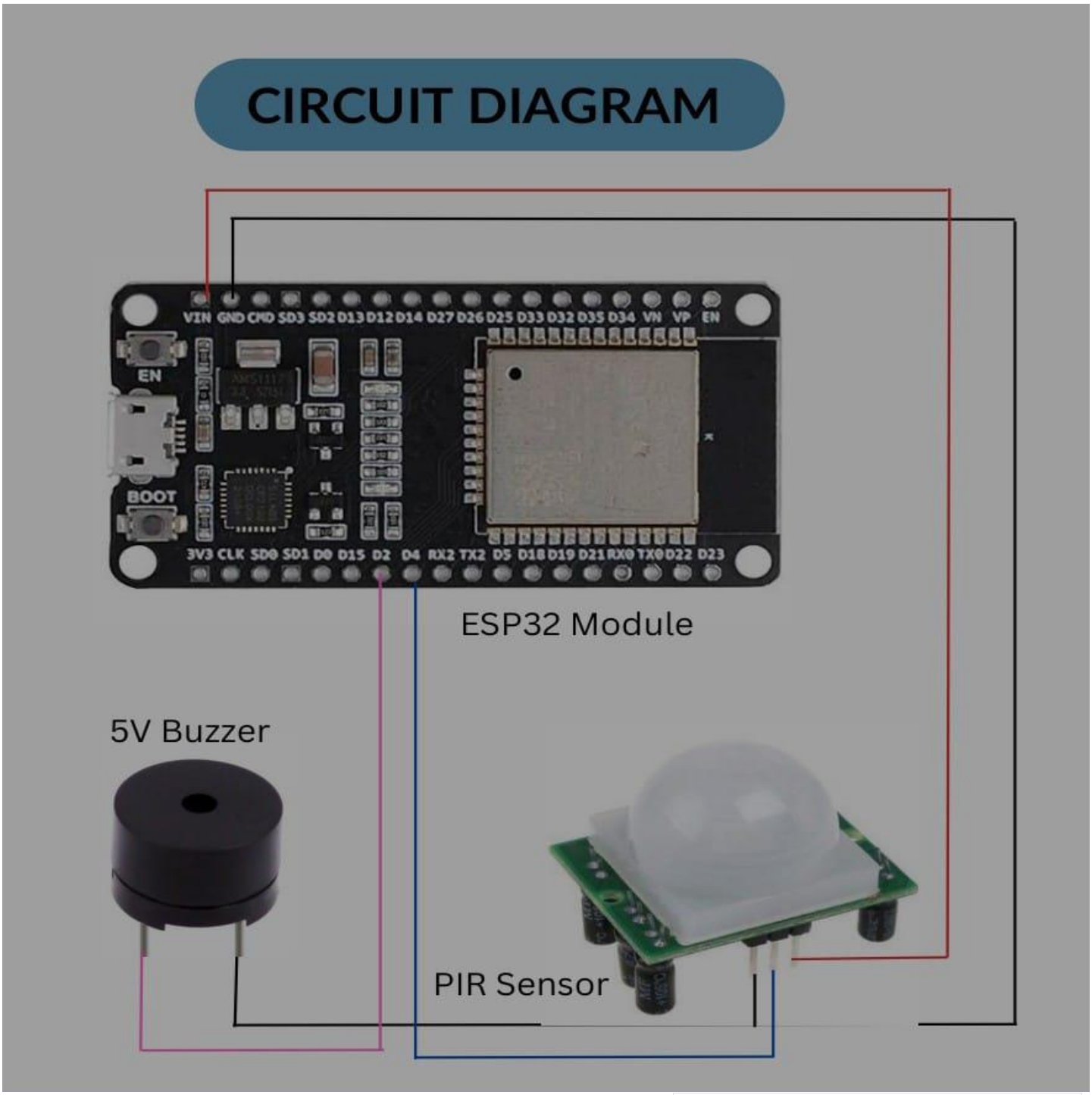
OTA (Over-The-Air) Updates: The ESP32 platform supports OTA updates, allowing users to remotely update firmware, apply security patches, and introduce new features without physically accessing the device. This feature simplifies maintenance, reduces downtime, and ensures that the security system remains up-to-date with the latest improvements and enhancements.

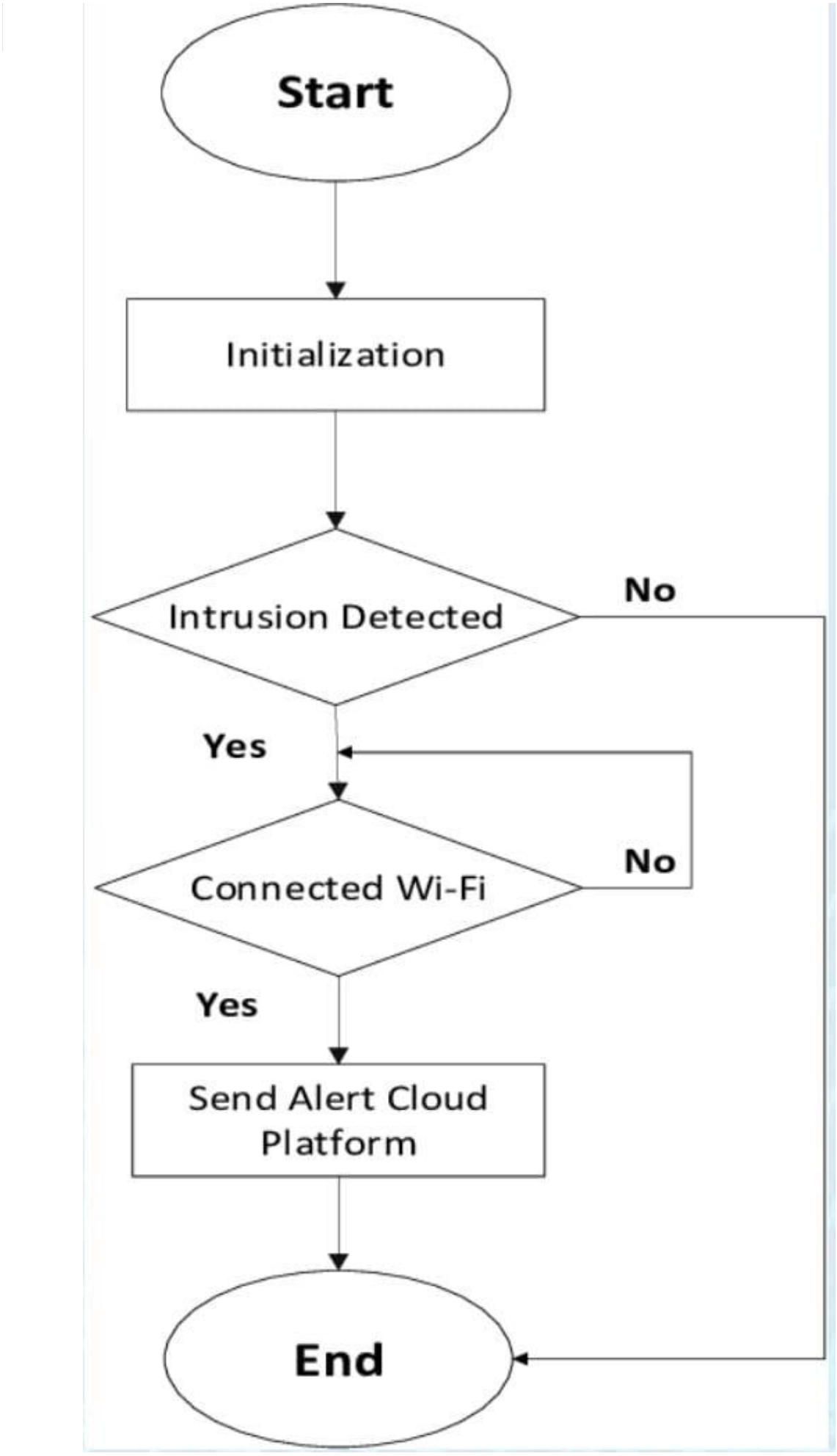
Integrated Microcontroller: The ESP32 integrates a powerful microcontroller with dual-core processing capabilities, providing ample computational power for running security algorithms, handling sensor data, and executing control logic efficiently.

Modularity and Scalability: The ESP32 architecture supports modular design principles, allowing users to expand and customize their security systems with additional components and functionalities as needed. This scalability enables users to adapt their security systems to evolving requirements, accommodate changes in property layout, and integrate new technologies seamlessly.

Data Encryption and Security Protocols: To ensure the security and integrity of data transmitted over the network, the ESP32 security system employs encryption protocols such as HTTPS and SSL/TLS. These protocols encrypt the communication between the microcontroller and the connected devices, preventing unauthorized access and tampering.

FIGURES/DIGRAMS




Start
Initialization
Intrusion Detected
No
Yes
Connected Wi-Fi
No
Yes
Send Alert Cloud Platform
End

METHODOLOGY

Alarm and Notification Mechanisms:

Implement alarm triggers and notification mechanisms to alert users in real-time when security breaches or abnormal events are detected.
Utilize audible alarms, visual indicators (LEDs), push notifications, email alerts, or SMS notifications to notify users and relevant authorities promptly.
Remote Monitoring and Control:

Develop a user interface, such as a web-based dashboard or a mobile application, to enable users to remotely monitor the security system status, view sensor data, and control system
Requirement Analysis:

Identify the specific security requirements and objectives of the system, including the type of threats to be addressed, the area to be monitored, and the desired response mechanisms.
Sensor Integration:

Select and integrate appropriate sensors such as motion sensors, door/window sensors, temperature sensors, smoke detectors, and other relevant sensors based on the security requirements.
Interface the sensors with the ESP32 controller using compatible communication protocols such as I2C, SPI, or GPIO.
Wireless Connectivity:

Configure the ESP32 module for Wi-Fi and/or Bluetooth connectivity to enable communication with other devices, the internet, and mobile applications.
Establish secure connections using encryption protocols (e.g., WPA2, TLS/SSL) to protect data transmission and ensure privacy.
Data Acquisition and Processing:

Continuously monitor sensor data to detect changes, events, or anomalies indicative of security breaches or unauthorized activities.
Process sensor data using built-in algorithms or custom logic implemented on the ESP32 microcontroller to analyze, filter, and interpret the data effectively.