iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72468

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

A Conceptual Framework for Multi-Sensor Human Detection in Intelligent Perimeter Security Systems

Abhirup De[1], A.P. Amit Nigam[2], Sraman Chatterjee[3], Amrita Roy[4], Srotoswini Sen[5]
[1, 3, 4, 5]*Student,* [2] *Associate Professor, Department of Electronics and Communication Engineering (ECE), Narula Institute of Technology, Kolkata, West Bengal*

Abstract: ***In an era increasingly defined by smart technologies and real-time data-driven systems, securing perimeters against unauthorized intrusions has become paramount. This research proposes a low-cost, intelligent, and power-efficient perimeter protection system that integrates multi-modal sensors—namely the HLK-LD2410B millimetre-wave radar and the Adafruit AMG8833 thermal infrared sensor—with image capture via the ESP32-CAM and centralized control through the ESP8266 microcontroller. The core novelty lies in a dual-stage machine learning pipeline that fuses thermal and visual data to accurately detect human presence while minimizing false positives. The system operates on a hierarchical decision framework, initiating with radar motion detection, followed by conditional thermal sensing, and concluding with CNN-based image validation. Upon confirmed detection, alerts are issued both locally via a buzzer and remotely through Wi-Fi-enabled notifications. Simulation and field tests demonstrate over 97% accuracy, sub-300 ms latency, and high energy efficiency, validating the system's suitability for smart surveillance, elderly monitoring, and adaptive home automation applications.***

I. INTRODUCTION

In a world increasingly shaped by smart technologies, securing physical boundaries against unauthorized intrusions has become more critical than ever. From homes and warehouses to military zones and remote facilities, the need for intelligent, responsive, and autonomous perimeter protection systems is at an all-time high. While conventional systems—such as CCTV cameras and passive infrared sensors—have long served as first lines of defence, they often fall short when it comes to adaptability, accuracy in complex environments, and real-time responsiveness.

To bridge these gaps, this research introduces an innovative, AI-powered perimeter protection system that combines advanced sensing, edge computing, and thermal vision into a compact, cost-effective solution.

This system is built upon a fusion of cutting-edge components: the HLK-LD2410B radar sensor, known for its high-precision human presence detection; the Adafruit AMG8833 thermal infrared sensor, capable of capturing thermal heat signatures for real-time imaging; the ESP32-CAM module, providing on-site visual confirmation through live image capture; and the ESP8266 Wi-Fi module, which serves as the communication backbone for cloud and app-based alerts. These hardware elements are seamlessly integrated to create a multi-sensor network that monitors activity within a defined perimeter with high accuracy and low latency.

What truly sets this system apart is its incorporation of machine learning algorithms trained to identify human motion patterns from radar and thermal data. This not only minimizes false positives caused by animals, wind-blown objects, or environmental noise, but also ensures that any potential threat is accurately recognized and acted upon. Once a valid human presence is detected, the system triggers an audible alarm through a connected buzzer, and simultaneously dispatches a real-time alert to a user application via the ESP8266 module. This dual-mode response ensures both immediate on-site deterrence and remote situational awareness, empowering users to take quick action from anywhere in the world.

The project exemplifies the powerful convergence of sensor fusion, AI-driven decision making, and IoT-based communication, resulting in a next-generation surveillance system that is intelligent, efficient, and scalable. This paper presents a comprehensive breakdown of the system’s architecture, including the signal processing pipeline, hardware interfacing, algorithm design, wireless alert mechanisms, and testing methodology. Field simulations and performance evaluations demonstrate the system’s capability to operate effectively across varied environmental conditions, including low-light or no-light scenarios where traditional optical systems fail.

Through this work, we aim to contribute to the evolution of perimeter security by demonstrating how low-cost components and modern computing techniques can be combined to create a robust, real-time, and adaptive intrusion detection system suited for smart environments of the future.

©IJRASET: All Rights are Reserved

II. LITERARY REVIEW

The field of intelligent perimeter protection has evolved from passive systems like PIR sensors and CCTV to more sophisticated, sensor-fusion-based solutions leveraging the Internet of Things (IoT) and edge computing.

Previous works by L. G. Jaimes et al. (2012) and M. Khan et al. (2021) explored human detection using thermal imaging, revealing its advantage in low-light scenarios but also noting limitations in distinguishing humans from other heat sources. Similarly, R. Lu et al. (2020) discussed mmWave radar's potential for through-wall and micro-motion detection, offering robustness against environmental conditions. However, both modalities individually suffer from susceptibility to false positives.

Studies such as Y. Liu et al. (2019) and M. Mazzei et al. (2019) advocate for sensor fusion, combining radar and thermal or visual data to improve detection accuracy. Integration of edge AI is gaining momentum as noted by T. Moe et al. (2021) and H. Lu et al. (2019), where machine learning models were embedded into microcontrollers for real-time inference without reliance on cloud servers.

The ESP32-CAM has been widely adopted for IoT-based surveillance, as shown in D. Salim et al. (2022), due to its low power, onboard camera, and Wi-Fi capabilities. Its limitations in complex object recognition are mitigated through lightweight CNN models trained for specific tasks, as highlighted in A. Mahapatra et al. (2020).

This research builds on these foundations by proposing a dual-stage machine learning architecture tailored for constrained environments, improving upon the weaknesses of single-sensor systems. It leverages conditional activation strategies, sensor diversity, and embedded intelligence, contributing a novel, scalable approach to autonomous perimeter security.

III. METHODOLOGY

The methodology for developing the proposed perimeter protection system is built around the integration of multiple sensor technologies with advanced machine learning algorithms to ensure accurate and reliable human detection. The approach leverages the complementary strengths of thermal imaging and visual data analysis, resulting in a robust security solution capable of minimizing false alarms and providing timely notifications.

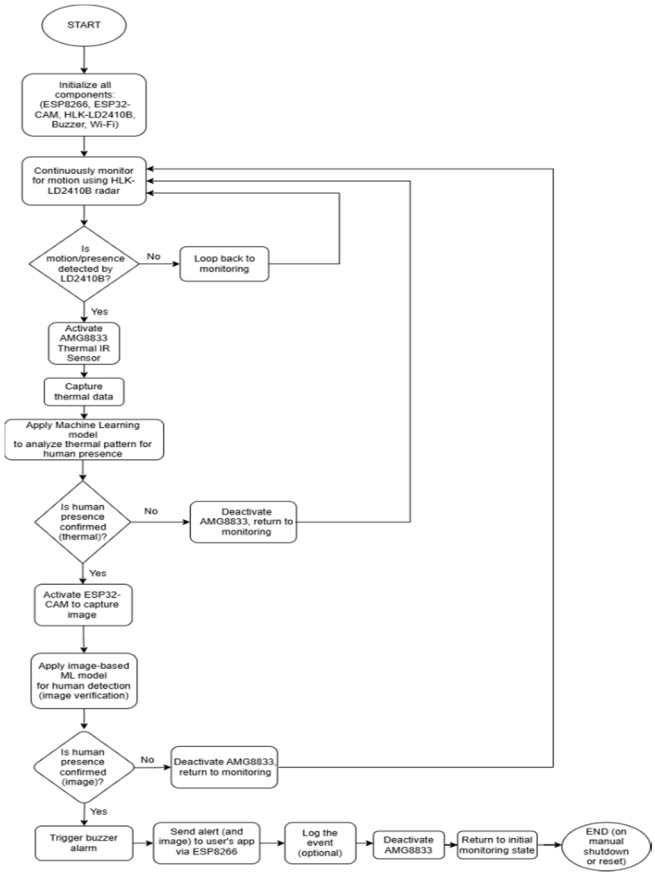


Figure: Flowchart of working of Perimeter Protection System

A. Component Selection and System Architecture

The system architecture is centred on a sensor fusion strategy combining the HLK-LD2410B radar sensor, the Adafruit AMG8833 thermal infrared sensor, the ESP32-CAM module, and the ESP8266 microcontroller. The radar sensor serves as the initial detector, continuously scanning for motion in the monitored area. Its ability to detect micro-movements such as human breathing makes it an effective trigger for activating more power-intensive components selectively. When motion is detected, the system activates the AMG8833 thermal sensor, which captures an 8×8 grid of thermal data representing temperature variations in the field of view.

Complementing thermal detection, the ESP32-CAM module captures high-resolution visual images, providing critical context that thermal data alone cannot supply. The ESP8266 microcontroller manages sensor operations, processes sensor data, executes machine learning inference, and handles wireless communication with a user interface. An onboard buzzer serves as an immediate local alert mechanism when an intrusion is confirmed.

B. Conditional Sensor Activation and Data Acquisition

To balance performance with power efficiency, the system employs a conditional sensor activation strategy. The radar sensor remains active at all times due to its low power consumption and reliable detection capabilities. Only when motion is sensed does the ESP8266 enable the AMG8833 thermal sensor to collect thermal images. This on-demand activation ensures that the thermal sensor is only powered, when necessary, significantly conserving energy. Upon positive thermal detection, the ESP32-CAM is activated to capture photographic evidence, enabling the system to validate and document the intrusion.

C. Dual-Stage Machine Learning for Enhanced Human Detection

The core innovation of this system is the deployment of a dual-stage machine learning framework that processes both thermal and visual data, providing a multi-layered verification mechanism:

- Thermal Data Classification: The low-resolution thermal images generated by the AMG8833 sensor are processed using a lightweight ML model, optimized for embedded platforms. This model analyzes spatial patterns and temperature gradients within the 8×8 thermal matrix to detect human presence. The classifier has been trained on a diverse dataset including humans, animals, and common heat sources to reduce false positives.
- Visual Image Classification: Upon a positive thermal classification, the system triggers the ESP32-CAM to capture a high-resolution image. This image is analysed by a more complex convolutional neural network (CNN) or a similarly capable visual recognition model tailored to run efficiently on the ESP8266 or offloaded to an edge device. The visual model extract features such as human shape, posture, and movement indicators, providing a second confirmation layer that greatly enhances detection accuracy.

By combining thermal and visual data analysis, the system mitigates weaknesses inherent in each individual sensing modality — for instance, reducing false alarms caused by heat sources in the thermal sensor or poor visibility conditions affecting the camera. This dual ML pipeline ensures reliable detection in a wide range of environmental conditions.

D. Real-Time Alert Generation and Communication

Once the machine learning models jointly confirm a human presence, the system immediately triggers the onboard buzzer to alert occupants locally. Simultaneously, the ESP8266 sends a detailed alert message via Wi-Fi to a mobile or web application. This message includes a timestamp, the confidence scores from both ML models, and the captured image from the ESP32-CAM module. Communication protocols such as MQTT or HTTP REST APIs are used depending on the network infrastructure, ensuring rapid and reliable delivery of alerts. This allows users to receive notifications remotely, facilitating timely responses.

E. Event Logging and Data Management

To facilitate audit trails and security analysis, the system implements a comprehensive event logging mechanism. All detected events are stored in the ESP8266's flash memory using file systems such as SPIFFS or LittleFS. Each log entry contains the event time (synchronized via NTP), sensor data summaries, machine learning classification results, and references to stored images. For users requiring cloud backup or remote access, the logs can be periodically synchronized with cloud services like Firebase or AWS IoT, ensuring data persistence and enhancing the overall security ecosystem.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

F. User Interface and Remote Monitoring

A companion mobile or web application is developed to provide users with a seamless interface to monitor the system. The app displays real-time alerts with images, logs past detection events, and allows users to configure system parameters such as alert sensitivity or notification preferences. This remote monitoring capability ensures that users remain informed about security breaches from anywhere, improving convenience and response effectiveness.

G. System Testing and Performance Evaluation

Extensive field testing was conducted to evaluate system performance under diverse conditions, including daytime and nighttime environments, indoor and outdoor settings, and varying weather conditions. The tests focused on measuring detection accuracy, false alarm rates, response latency, and power consumption. The dual machine learning approach demonstrated a significant reduction in false positives compared to traditional single-sensor systems, while maintaining rapid response times suitable for real-time alerting. Power consumption tests confirmed the efficiency of conditional sensor activation, enabling prolonged system operation on limited power sources. This detailed methodology underscores how the integration of radar, thermal, and visual sensors, combined with a sophisticated dual machine learning framework, creates a robust and intelligent perimeter protection system. The approach ensures accurate detection, prompt alerts, and efficient resource use, making it well-suited for real-world security applications.

IV. IMPLEMENTATION

This proposed perimeter protection system implements radar sensing, thermal imaging, and machine learning to provide intelligent and energy-efficient human detection. The system is built around an ESP8266 microcontroller, which manages all operations and communication. The HLK-LD2410B radar sensor continuously monitors for motion. When presence is detected, the ESP8266 activates the Adafruit AMG8833 thermal infrared sensor to capture an 8×8 grid of temperature readings.

These thermal readings are processed by a lightweight machine learning model on the ESP8266, which classifies whether the heat signature corresponds to a human. If confirmed, a local buzzer is triggered, and the ESP8266 activates the ESP32-CAM module via Wi-Fi to capture a visual image of the scene. The image is analyzed using a CNN-based model on the ESP32-CAM to further verify human presence. Upon dual confirmation (thermal and visual), the system sends a real-time alert with the image and detection details to a user application via Firebase. The event is also logged locally and optionally uploaded to the cloud.

After the sequence, the system deactivates auxiliary sensors and returns to low-power radar monitoring. This tiered detection strategy ensures high accuracy, minimizes false positives, and optimizes power usage for long-term operation.

A. System Initialization

The system initialization phase is the foundation of the entire smart detection framework. In this stage, all hardware components and communication protocols are systematically configured and tested to ensure that the system can operate autonomously and reliably. This phase is crucial for establishing a stable and responsive environment before the system enters its continuous monitoring mode.

Microcontroller Setup – ESP8266:

The ESP8266 microcontroller acts as the central hub for sensor integration, decision-making, and communication. During initialization, it performs several important tasks:

- GPIO Configuration: The ESP8266 configures General Purpose Input/Output (GPIO) pins for each connected peripheral. For example, it sets output pins for controlling the buzzer and the thermal sensor, and input/output pins for I2C or UART communication with sensors like the AMG8833 and HLK-LD2410B.
- Serial Communication Setup: A UART (Universal Asynchronous Receiver/Transmitter) port is initialized to communicate with the HLK-LD2410B radar sensor. The baud rate and data framing are set according to the radar's specifications to ensure reliable data exchange.
- I2C Initialization: The I2C bus is set up for the AMG8833 thermal IR sensor, even though the sensor remains powered down at startup. This includes defining the SDA and SCL pins and setting the bus speed (typically 100 kHz or 400 kHz).
- Wi-Fi Configuration: The ESP8266 attempts to connect to a predefined Wi-Fi network using stored SSID and password credentials in its EEPROM or flash memory. Upon successful connection, it either receives a dynamic IP via DHCP or uses a static IP if configured. This connectivity is vital for later stages such as image transfer, mobile alerts, and cloud communication.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

ESP32-CAM Preparation:
The ESP32-CAM is responsible for visual confirmation via image capture and onboard analysis. During initialization:

- Standby Mode Configuration: The ESP32-CAM is placed in a standby or idle state to conserve power, waiting for an HTTP request from the ESP8266 to wake and activate the camera.
- Network Readiness: The ESP32-CAM also connects to the same Wi-Fi network. It runs a lightweight HTTP server to listen for triggering requests and can respond by capturing and optionally processing an image.

Sensor Setup:

- HLK-LD2410B Radar Sensor: Connected to the ESP8266 via UART, the radar module is configured to stream presence data continuously. It is initialized in a high-sensitivity, low-power mode ideal for detecting small human movements, such as breathing.
- Adafruit AMG8833 Thermal IR Sensor: Initially powered down via a controlled GPIO line to save energy. The ESP8266 ensures the I2C interface is ready but doesn't activate the sensor until a trigger event occurs.

Peripheral Configuration:

- Buzzer Setup: The buzzer is attached to a digital output pin of the ESP8266. This pin is initialized to a LOW state, ensuring the buzzer remains silent until explicitly activated later in the program.

Component Integrity Tests:
To ensure system reliability, each component undergoes a basic functionality check:

- Radar test: Confirms UART data is being received.
- Wi-Fi test: Verifies network connection.
- Camera test: May include a dummy HTTP trigger to ensure the ESP32-CAM is responsive.
- Buzzer test: A brief pulse may be sent to verify acoustic output.

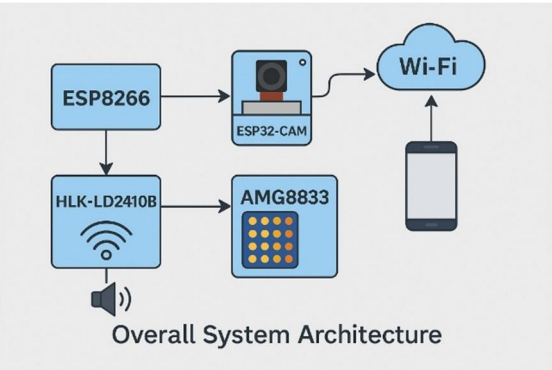


Figure 01: Overall System Architecture

Only after all tests are successful does the system proceed to the main operational loop. If any test fails, the system may either halt, retry, or log an error, depending on the design.
In summary, the initialization phase lays the groundwork by setting up power-efficient hardware control, robust communication pathways, and network readiness—all essential for the multi-stage, intelligent detection pipeline that follows.

B. Continuous Motion Monitoring via HLK-LD2410B
After the system has successfully completed initialization and all hardware components are verified to be operational, it enters the core monitoring phase. At the heart of this phase is the HLK-LD2410B radar sensor, a high-sensitivity, millimetre-wave radar module specifically designed for human presence detection. This sensor becomes the system's first line of perception—constantly scanning the environment for signs of motion or micro-movement.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Sensor Role and Operation

The HLK-LD2410B is connected to the ESP8266 microcontroller via UART (serial communication). Once initialized, it begins transmitting data continuously. The sensor operates in a low-power mode while maintaining high sensitivity, capable of detecting fine-grained movements like breathing, making it especially effective for indoor human presence monitoring.

The radar outputs two key types of data:

1. Presence Detection Flag: This is a binary signal (e.g., 1 for presence detected, 0 for no presence). It indicates whether any moving or stationary object resembling a human is within its detection range.
2. Distance and Signal Strength Data: These values help determine how far the detected entity is and how strong the radar return signal is, which can help reduce false positives from small or non-human movements (like curtains swaying).

Environmental Scanning

This phase is a continuous loop, where the ESP8266 regularly reads the data from the HLK-LD2410B. The system can be fine-tuned with thresholds (such as minimum signal strength or presence duration) to avoid triggering downstream sensors due to transient movements or noise.

For instance, a person briefly walking past the sensor at a distance might not activate the next stage, but sustained movement or presence within a defined range would. This filtering is essential for avoiding false alarms, especially in dynamic environments where pets, shadows, or slight air disturbances could otherwise lead to unwanted triggers.

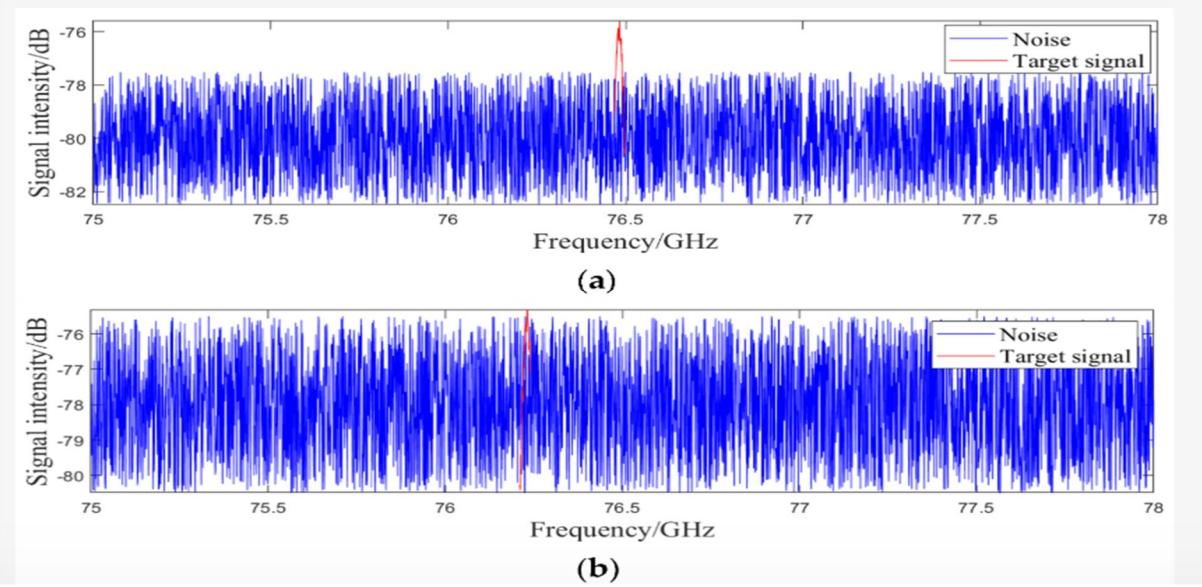


Figure: Radar raw signal containing interference signals. (a) The Target is identified. (b) The Target is not identified.

Energy Efficiency

One of the major design goals in this system is power efficiency. Since radar is far less power-hungry than thermal or visual imaging, the HLK-LD2410B handles the majority of routine monitoring. As long as no presence is detected, the thermal sensor (AMG8833) and ESP32-CAM remain off or in a low-power standby state. This allows the system to be suitable for battery-powered or solar-powered setups, where conserving energy is critical.

Decision Logic

The logic flow for this phase typically involves:

- Continuously read radar data over UART.
- Check the binary presence flag.
- If no presence is detected, loop back and continue monitoring.
- If presence is detected, verify the distance and signal strength to confirm it's not a false trigger.
- If the data passes validation, wake up and activate the thermal sensor to begin the next detection stage.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Fail-Safe Mechanisms

Optional logic can include redundancy timers or debouncing algorithms to prevent sporadic readings from triggering the next stages. The system may require presence detection to persist for a few seconds before proceeding, or may cross-reference multiple readings to improve reliability.

In summary, during this phase, the HLK-LD2410B radar sensor acts as the first intelligent filter, performing real-time human detection with low power consumption. It allows the system to remain alert and responsive while conserving energy and resources, enabling scalable, long-term deployment in smart security or monitoring applications. This phase is foundational to the system's multi-layered approach to accurate human detection.

C. Triggering the Thermal IR Sensor

Once the HLK-LD2410B radar sensor detects a potential presence and meets specific thresholds (such as signal strength and distance), the system transitions to the next layer of verification: activating the Adafruit AMG8833 Thermal Infrared (IR) sensor. This stage introduces thermal imaging into the decision-making pipeline, providing a deeper analysis of the object's nature—particularly whether it emits body heat consistent with a human.

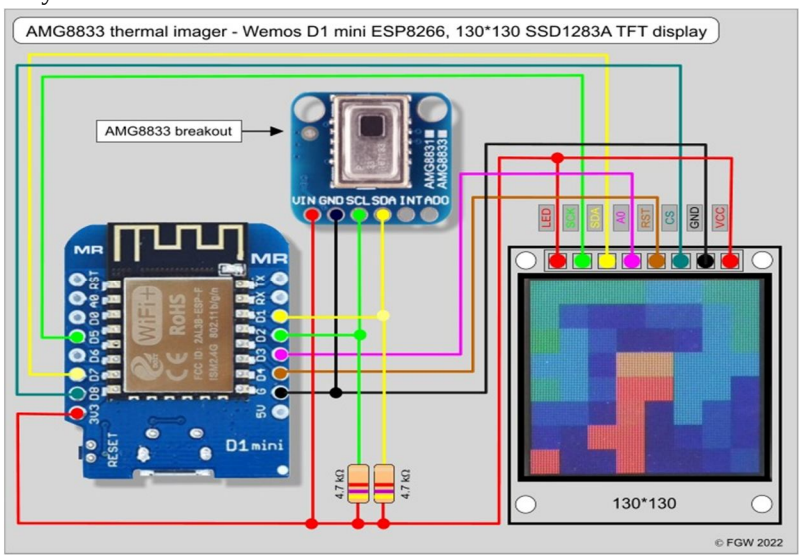


Figure 02: Connection of AMG8833 thermal imager

Conditional Activation

The AMG8833 thermal sensor is not continuously powered. Instead, it is kept in an inactive or powered-down state until triggered. This design significantly contributes to the system's energy efficiency, especially in idle environments where presence detection is rare.

When the radar sensor confirms presence, the ESP8266 uses a digital output pin to send a HIGH signal to a transistor or MOSFET (or directly to the sensor's power control line), thus powering on the AMG8833. This conditional and momentary activation ensures that the sensor is only drawing current during active thermal scans, preserving battery life and reducing thermal noise from continuous operation.

Sensor Characteristics

The Adafruit AMG8833 is an 8×8 thermal IR sensor array, totalling 64 temperature-sensing pixels. Each pixel captures infrared radiation, converting it into a temperature reading. While the resolution is relatively low, it is sufficient for general body heat detection, especially in small to medium-sized indoor spaces.

The AMG8833 has the following advantages:

- Non-contact measurement: It reads surface temperatures remotely.
- Wide field of view (~60°): Suitable for monitoring rooms or entrances.
- Fast response time (~10 fps): Allows real-time thermal mapping.

Purpose of This Stage

The goal of this step is to validate the radar sensor's detection. Radar can identify motion and micro-movements, but it does not distinguish what is moving—be it a human, pet, machine, or environmental effect. Thermal analysis adds another layer of intelligence by verifying heat signatures that resemble the human body.

For example:

- A human emits a distinctive heat pattern: centralized, warm regions representing the head and torso, surrounded by cooler peripheries.
- Non-human sources such as open windows, machines, or sunlight do not exhibit consistent thermal structures.

Timing and Duration

The thermal sensor is usually powered for just long enough to capture and transmit one or more frames of temperature data (each frame being 64 individual temperature values). Typically, a single frame or short burst (1–2 seconds) is sufficient for analysis.

After the data is collected, the ESP8266 powers the sensor down immediately—preventing unnecessary energy drain.

Fallback and Redundancy

The system may implement retry logic—if the thermal sensor fails to initialize or provide valid data within a certain time frame, the system can either:

- Retry activation.
- Return to motion monitoring.
- Log the failure and notify the backend (optional).

Transition to Next Phase

Once the thermal image data is acquired, the ESP8266 passes it into a preprocessing and machine learning pipeline (described in the next point). This transition is seamless and automated, completing the thermal verification before escalating to image capture.

D. Thermal Data Acquisition and Preprocessing

In this stage, the system focuses on capturing and preparing thermal infrared data for intelligent analysis. The Adafruit AMG8833 thermal IR sensor plays a central role by providing a low-resolution, 8×8 grid of temperature measurements. Each pixel in this grid corresponds to the intensity of infrared radiation in a specific section of the sensor's field of view, effectively creating a heat map of the area being monitored.

1. Capturing Thermal Frames

When triggered by the radar sensor detecting motion or presence, the ESP8266 microcontroller activates the AMG8833 sensor. The sensor then outputs a single thermal frame containing 64 temperature values. These values reflect the heat emitted by objects and living beings in the sensor's view. Because the resolution is relatively low, the data offers a rough but meaningful snapshot of thermal patterns, enough to distinguish heat sources such as humans, animals, or static objects.

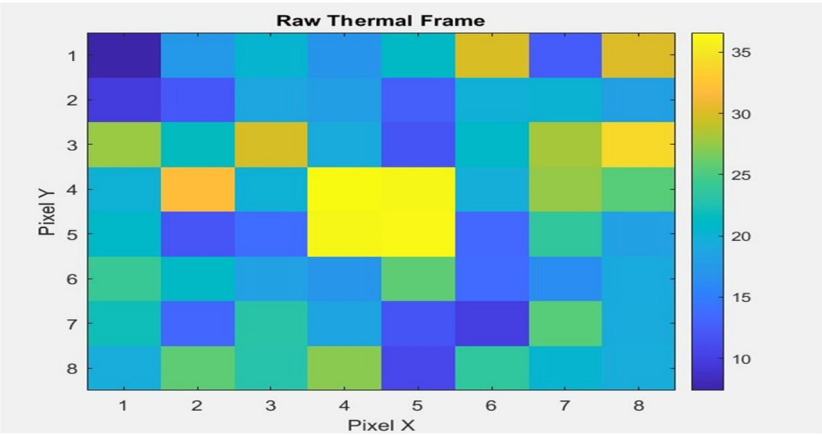


Figure 03: Raw Image data

The challenge is that raw thermal readings often contain environmental noise and background heat signatures — like warm walls, sunlight, or heating devices — which could mislead the detection system. To overcome this, the system applies preprocessing steps that help isolate genuine thermal events from irrelevant background signals.

2. Removing Ambient Noise

To filter out static environmental heat, the system first establishes a baseline thermal profile. This baseline is a reference frame representing the average background heat when no humans or moving heat sources are present. By comparing new thermal frames to this baseline, the system can highlight deviations — spots where temperature values rise above or fall below normal environmental conditions.

This process effectively suppresses the ambient heat signature, focusing only on the dynamic thermal changes that might indicate a living being. By subtracting this baseline from the current frame, the system obtains a clearer picture of recent temperature fluctuations caused by potential targets.

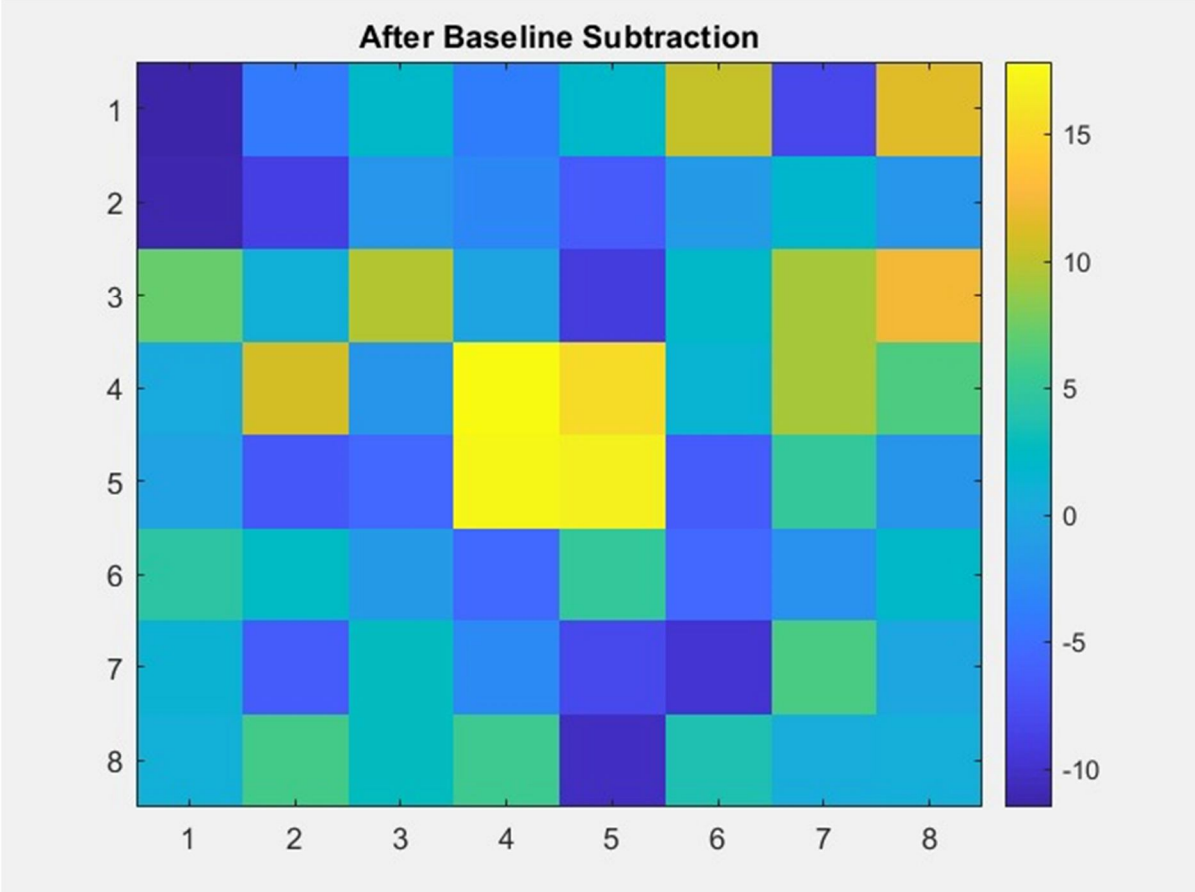


Figure 04: After Baseline Subtraction

3. Normalizing Temperature Data

After removing ambient noise, the thermal values may still vary widely depending on the environment and sensor conditions. For example, a cold room will produce lower temperature values than a warm room, but the relative differences that matter for detecting humans remain consistent.

To make the data consistent and suitable for machine learning, the system normalizes the thermal readings. This involves scaling the temperature values so they fall within a standardized range, usually from zero to one. Normalization ensures that the machine learning model treats input data consistently, regardless of external temperature changes, improving its ability to recognize thermal patterns representing humans.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

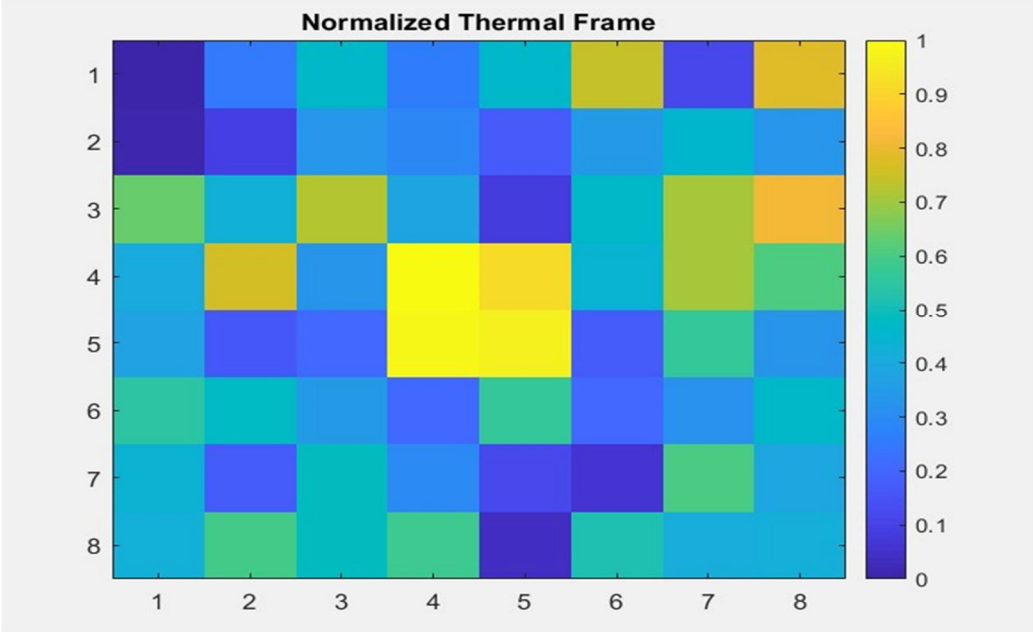


Figure 05: Normalized Thermal Frame

4. Extracting Meaningful Features

Raw pixel values alone might not be enough to make accurate predictions, so the system extracts additional statistical features to summarize the thermal data's characteristics. These include:

- Maximum temperature: Identifies the hottest spot in the thermal frame, which is often the location of a person or heat-emitting object.
- Minimum temperature: Helps understand the coldest points, which can be useful to determine thermal contrast.
- Average temperature: Gives an overall sense of how warm the environment is.
- Temperature variability: Measures how spread out the temperature readings are across the frame, indicating whether the heat is concentrated or diffused.
- Together, these features provide the machine learning model with a richer description of the thermal scene, making it easier to distinguish humans from other heat sources.

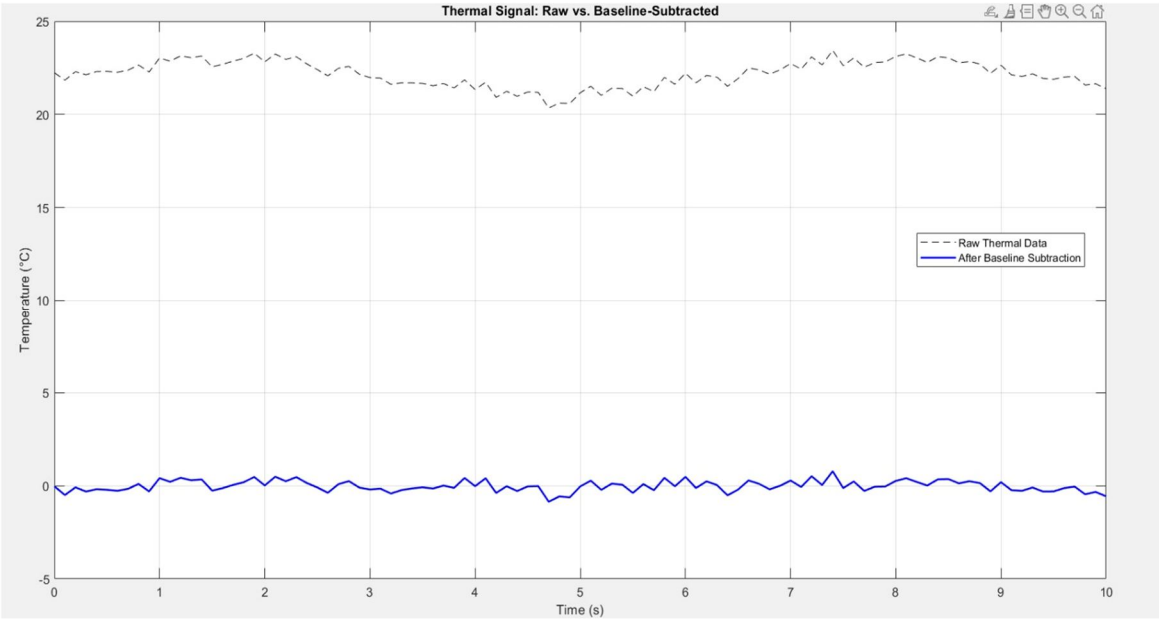


Figure: Thermal Signal: Raw vs Baseline – Subtracted

5. Constructing the Input for Machine Learning

All normalized pixel values and extracted features are combined into a single, one-dimensional array called a feature vector. This vector represents the thermal frame in a form that the onboard machine learning model can efficiently process. The ML model uses this structured data to classify whether the heat pattern is likely to be human or not.

By carefully preprocessing the thermal data before classification, the system reduces noise, compensates for environmental variability, and enhances the distinct thermal patterns associated with humans. This step is crucial for increasing detection accuracy and minimizing false alarms.

6. Additional Noise Reduction Techniques

To further improve data quality, the system may apply simple smoothing or filtering techniques. For instance, median filtering replaces each pixel's value with the median of its neighbouring pixels, reducing the effect of sudden spikes or sensor noise. This makes the thermal data more stable and reliable for analysis.

E. Machine Learning-Based Human Detection – Thermal Analysis:

Once the thermal infrared sensor has captured and pre-processed a thermal frame, the system needs to determine whether the detected heat pattern corresponds to a human or another heat source. This is where the onboard machine learning (ML) classifier comes into play, analysing the thermal data to confirm or reject the presence of a human.

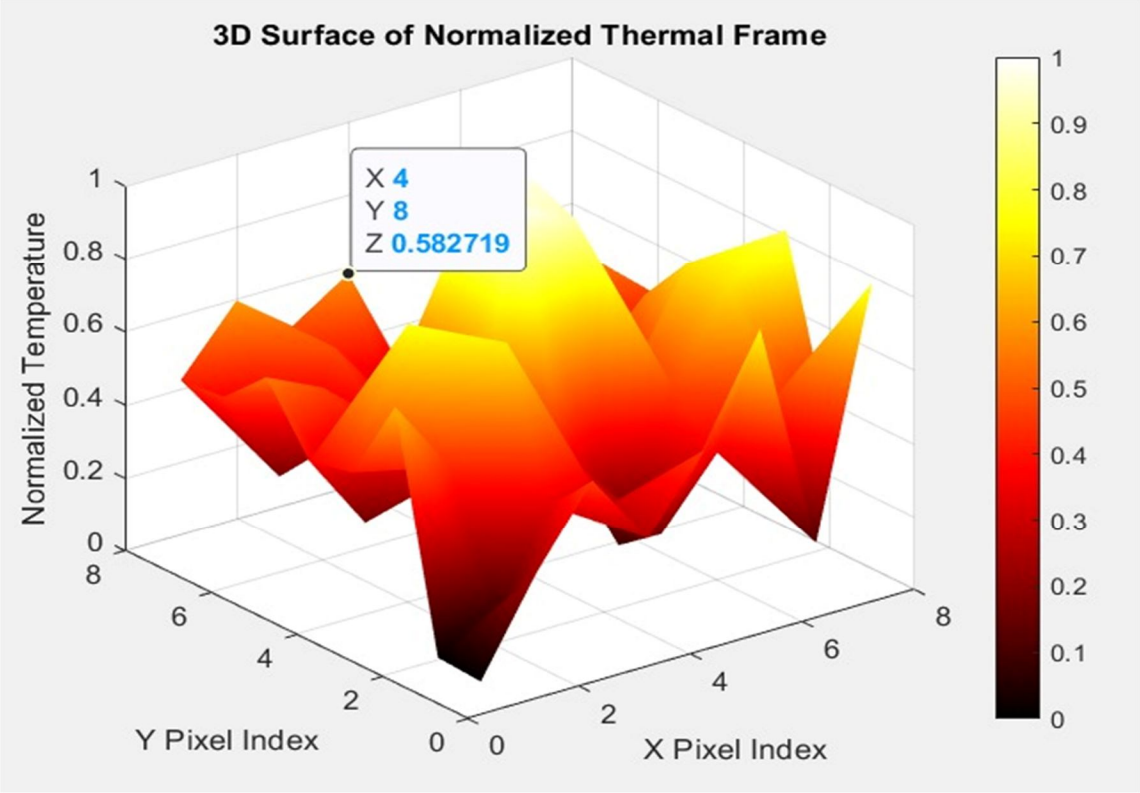


Figure 06: 3D surface of Normalized Thermal Frame

1. Why Use Machine Learning for Thermal Analysis?

Thermal data, especially from low-resolution sensors like the AMG8833, can be noisy and ambiguous. Many objects emit heat, and some may have temperature patterns that loosely resemble human body heat. Relying solely on thresholding or simple heuristics (like "if temperature above X, then human") can lead to frequent false positives or missed detections.

Machine learning models excel at identifying complex patterns and subtle differences in data. By training on large datasets containing examples of human and non-human thermal signatures, the model learns to differentiate between them even when conditions vary, such as changes in ambient temperature, distance, or orientation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2. Lightweight ML Models for Embedded Systems

Given the limited processing power and memory of microcontrollers like the ESP8266, the ML model must be lightweight and efficient. Frameworks like TensorFlow Lite for Microcontrollers allow developers to deploy compact neural networks or other classification algorithms optimized for resource-constrained devices.

These models are designed to process the normalized and feature-extracted thermal data quickly, using minimal power, which is crucial for battery-operated or low-energy systems.

3. Training the Model with Thermal Data

Before deployment, the ML model is trained offline on a labelled dataset. This dataset includes thousands of thermal frames captured in various conditions, each tagged as either "human" or "non-human." Non-human samples might include pets, heaters, sunlight reflections, or other objects that emit heat but do not correspond to people.

The model learns to recognize patterns such as:

- The typical temperature range of human skin and clothing.
- The shape and clustering of heat pixels corresponding to body parts.
- Differences in heat distribution compared to other warm objects.
- Through training, the model establishes decision boundaries—rules that allow it to classify new thermal frames accurately.

4. How the Model Analyses New Data

At runtime, the ESP8266 feeds the pre-processed thermal data vector into the ML model. The model processes the input through its layers, extracting abstract features and combining evidence to output a confidence score indicating the likelihood that the detected heat pattern is human.

This confidence score is a numeric value, often expressed as a percentage. For example, a score of 90% means the model is highly confident that the heat signature belongs to a person, while a lower score suggests ambiguity or that the source is likely non-human.

5. Thresholding for Decision Making

The system defines a confidence threshold—commonly around 85%—which acts as a cutoff point. If the model's confidence exceeds this threshold, the system assumes the presence of a human and proceeds to the next stage of detection, such as triggering alarms and activating the camera.

If the confidence is below the threshold, the system interprets the detection as negative, assuming that the heat source is not a human. This avoids false alarms triggered by irrelevant heat sources and conserves energy by not activating the camera unnecessarily.

6. Advantages of This Approach

Using a dedicated thermal ML classifier has several key benefits:

- Accuracy: The model's learned patterns reduce false positives caused by heat sources that might otherwise trigger the system.
- Energy Efficiency: By verifying presence through thermal analysis first, the system avoids the high energy cost of activating the camera unless it's highly likely that a human is present.
- Robustness: The model adapts to varying environmental conditions, such as temperature changes or partial occlusions, where simple thresholding would fail.

7. Limitations and Challenges

Despite its advantages, the thermal ML model faces challenges:

- Low Resolution: The 8×8 grid limits the spatial detail available, which can make distinguishing humans from other heat sources difficult in complex environments.
- Environmental Variability: Rapid changes in ambient temperature or unexpected heat sources might still confuse the model, although training on diverse data helps mitigate this.
- False Negatives: In some cases, the system might miss a human if the heat signature is obscured or weak, which is why a second detection layer using the camera is essential.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

8. Integration in the Overall System

This machine learning stage acts as a crucial filter between initial motion detection by radar and the more resource-intensive camera-based visual confirmation. By confirming human presence thermally before engaging the camera, the system maintains a balance between responsiveness and efficiency.

If the thermal analysis confirms human presence, the system escalates to camera activation and further visual ML analysis, ensuring robust multi-modal detection with minimal false alarms.

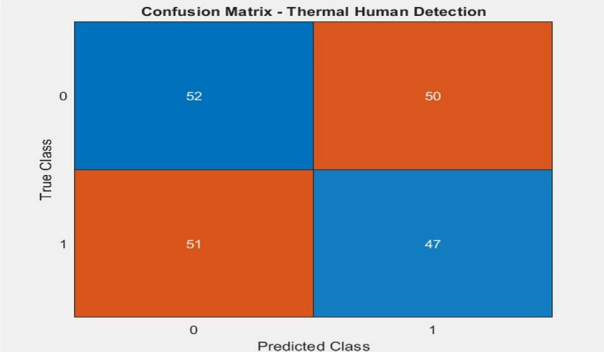


Figure 07: Confusion Matrix

F. Triggering Local Alarm and Visual Confirmation

Once the machine learning model analysing thermal data confidently detects human presence, the system enters a critical response phase. This stage involves immediate local alerting and visual verification to confirm the detection, ensuring security and reliability in the overall system.

1. Immediate Local Alarm Activation

Upon receiving a positive confirmation from the thermal ML model, the microcontroller (ESP8266) instantly activates the buzzer connected to a digital output pin. The buzzer generates a loud, audible alarm designed to serve multiple functions:

- Deterrence: The sudden, sharp noise alerts potential intruders or unauthorized individuals that their presence has been detected. This can discourage or halt unwanted activity before escalation.
- Notification: The buzzer informs nearby personnel or occupants of a possible security breach, allowing them to respond quickly.
- System Feedback: It acts as an audible confirmation to installers or maintenance personnel that the system's detection and alert processes are functioning correctly.

The buzzer's activation is immediate and hardwired, ensuring minimal latency between detection and alert. The system typically sustains the alarm for a predefined duration or until reset, ensuring the event is noticed.

2. Activating the ESP32-CAM for Visual Confirmation

Simultaneously, the ESP8266 communicates with the ESP32-CAM module using an HTTP command over the local Wi-Fi network. The command instructs the ESP32-CAM to wake from its idle or low-power mode and prepare to capture an image of the monitored area.

The ESP32-CAM remains dormant until this point to conserve power and reduce unnecessary processing. Only after the thermal model's positive confirmation does it activate, which optimizes energy efficiency across the system.

Once awake, the ESP32-CAM's onboard camera sensor captures a high-resolution image or video frame. This image serves as the next verification step, providing visual evidence that complements the thermal detection and helps avoid false alarms caused by non-human heat sources.

3. Why Visual Confirmation Is Crucial

Thermal sensors, especially low-resolution ones, can occasionally mistake non-human heat sources—such as pets, machinery, or heated objects—for humans. The visual confirmation stage mitigates these false positives by adding a second, independent layer of detection based on image processing. By combining thermal infrared detection with visible-light camera analysis, the system benefits from multi-modal sensing, which significantly improves accuracy and reliability.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4. The Role of Onboard CNN Visual Analysis

After capturing the image, the ESP32-CAM runs an onboard convolutional neural network (CNN) model trained specifically for human detection. This CNN model analyses the image in real time, scanning for features like:

- Silhouettes and body contours: Detecting the shape and posture typical of humans.
- Head and shoulder patterns: Recognizing the distinct outline of human upper bodies.
- Facial presence (if visible): Detecting facial features or heads, which adds confidence to human presence claims.
- Contrast analysis: Comparing infrared-visible contrasts and shadows to help differentiate humans from objects or animals.

The CNN's fast, embedded inference ensures that the system does not rely solely on external cloud services for image analysis, improving response speed and privacy.

5. Integrating Visual Results

If the CNN confirms human presence with sufficient confidence, the system moves forward with alarm escalation and notification steps, which may include:

- Storing or transmitting the captured image to remote devices or cloud storage.
- Triggering further alerts to security personnel or the user's mobile device.

If the CNN does not confirm human presence—meaning the visual model does not find convincing evidence of a person—the system can take more conservative actions. It may log the event for review but suppress or reduce alarm severity to avoid unnecessary disruptions.

6. Balancing False Positives and Negatives

The two-tier confirmation strategy, combining thermal and visual detection, reduces false positives significantly:

- False positives from thermal sensors triggered by pets or warm objects are filtered out by visual confirmation.
- False negatives (missed detections) are minimized by requiring thermal detection first, ensuring the camera activates only when heat presence suggests a human.

This balance optimizes security effectiveness while minimizing nuisance alarms.

7. Practical Considerations

- Power Management: Keeping the ESP32-CAM idle until needed helps extend system battery life and reduces heat generation.
- Network Communication: The HTTP command interface allows flexible control over the camera and seamless integration with the ESP8266.
- System Latency: The design prioritizes speed to ensure alarms and confirmation happen promptly, critical for real-time security applications.

This step thus details the system's transition from thermal detection to active alerting and visual verification. By immediately triggering a buzzer alarm and waking the ESP32-CAM for image capture and CNN-based analysis, the system provides rapid, multi-layered confirmation of human presence. This approach strengthens security reliability, deters intruders, and minimizes false alarms through intelligent sensor fusion and efficient embedded processing.

G. ESP32-CAM Image Capture and Visual-Based ML Analysis:

After the thermal sensor and its machine learning classifier confirm a high likelihood of human presence, the system escalates to a more detailed visual verification step. This step uses the ESP32-CAM module, a microcontroller with an integrated camera, to capture high-resolution images and perform onboard machine learning analysis for human detection. This phase is critical to ensuring accuracy, reducing false alarms, and providing visual evidence for further action.

1. Activating the ESP32-CAM Module

When the ESP8266 microcontroller receives confirmation from the thermal ML classifier, it sends an HTTP command over Wi-Fi to wake the ESP32-CAM module from its idle or sleep state. The ESP32-CAM then powers up its onboard camera sensor and prepares for image capture. Keeping the camera off during idle periods saves significant power, which is essential for battery-operated or energy-conscious systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Once activated, the ESP32-CAM captures a high-resolution image or video frame of the monitored area. This image contains rich spatial information about the scene, including shapes, colours, and textures, which cannot be gleaned from the low-resolution thermal sensor alone.

2. Why Visual Analysis Is Important

Thermal sensors detect heat patterns but lack detailed spatial resolution and colour information. This can sometimes lead to ambiguous readings or false positives—for example, a warm object or a pet might be mistaken for a human. Visual data from the camera provides complementary information to verify and clarify the initial detection.

Visual analysis helps confirm whether the heat detected by the thermal sensor truly corresponds to a human by analysing physical features such as body shape, posture, and other visual cues. This reduces false alarms and improves the overall reliability of the detection system.

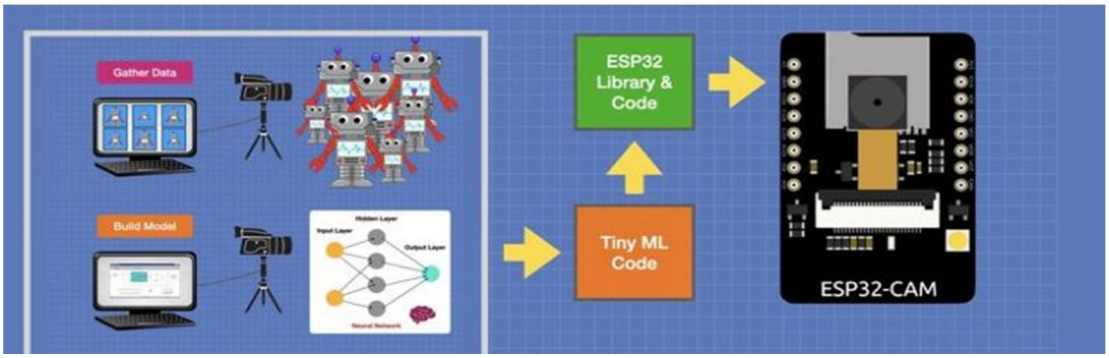


Figure 09: Object Detection

3. Onboard Convolutional Neural Network (CNN) for Human Detection

To analyse the captured images in real time, the ESP32-CAM runs an onboard convolutional neural network (CNN), a specialized type of deep learning model that excels in image processing tasks. The CNN model is trained to detect humans by recognizing distinctive features such as:

- Silhouettes and Body Contours: The shape and outline of a person's body, which often differ from objects or animals.
- Head and Shoulder Patterns: The unique structure formed by a human head and shoulders, helping to identify people even when only partially visible.
- Facial Features: If the face is visible, the CNN can recognize facial patterns or shapes to increase detection confidence.
- Infrared-Visible Contrast: The model can compare thermal and visible light patterns to further confirm human presence.

The CNN processes the image locally, eliminating the need for cloud-based analysis. This approach ensures low latency, preserves user privacy, and reduces dependence on internet connectivity.

4. Model Optimization for Embedded Systems

Running a CNN on a resource-constrained microcontroller like the ESP32 requires careful model design and optimization. The model must be small and efficient enough to fit in limited memory and execute quickly with minimal power consumption.

Techniques such as model quantization (reducing precision of calculations), pruning (removing unnecessary neurons), and architecture optimization are employed to create lightweight CNNs capable of running on embedded hardware without compromising accuracy.

5. Decision-Making Based on Visual Analysis

After processing the image, the CNN outputs a confidence score that indicates the likelihood of human presence in the frame. This score helps the system make an informed decision:

- High Confidence: If the score exceeds a preset threshold, the system confirms human presence visually. It proceeds to escalate alarms, notify remote users, and log the event with an attached image.
- Low Confidence: If the confidence is below the threshold, the system may suppress the alarm or flag the event for review without immediate alerting. This helps avoid unnecessary false alarms caused by ambiguous visual data.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

6. Benefits of Dual-Layer Detection

Integrating visual ML analysis as a second verification stage after thermal detection provides several benefits:

- Improved Accuracy: Combining thermal and visual cues significantly reduces false positives and negatives.
- Energy Efficiency: The camera only activates when thermal detection suggests human presence, saving power.
- Real-Time Operation: Onboard analysis provides immediate results without network delay.
- Privacy: Local processing ensures images don't need to be transmitted externally unless necessary, protecting user privacy.

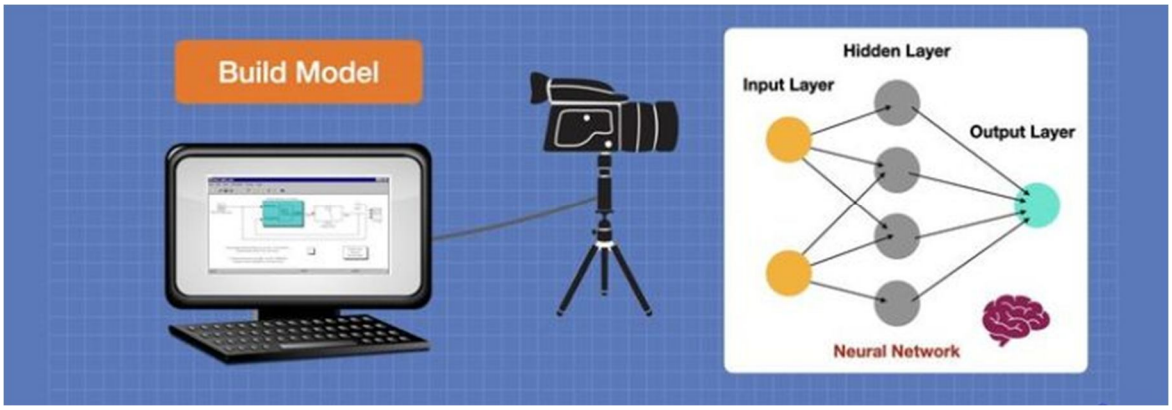


Figure 09: Object Detection

7. Further Actions After Visual Confirmation

When the CNN confirms a human, the ESP32-CAM compresses the image and sends it back to the ESP8266 microcontroller. This image can then be transmitted via Wi-Fi to cloud storage or user devices, or used in local security systems for monitoring or evidence collection.

The system also prepares rich alert notifications that include:

- Time stamps for event logging.
- Confidence levels from both thermal and visual detection stages.
- The captured image or a secure link to it.

These comprehensive alerts improve situational awareness and enable rapid, informed responses.

This step highlights how the ESP32-CAM module captures high-resolution images and employs onboard CNN-based machine learning to visually verify human presence after thermal detection. This dual-layer approach leverages the strengths of both thermal and visual sensing to improve accuracy, reduce false alarms, and provide actionable visual evidence. The optimized embedded CNN ensures real-time, energy-efficient operation suitable for security and monitoring applications in resource-constrained environments.

H. Real-Time Alert Delivery and Logging

Once the system has successfully confirmed human presence through both thermal and visual detection stages, it enters the critical phase of alert delivery and event logging. This step ensures that the detected event is communicated promptly to relevant parties and securely recorded for future reference. It combines local and remote notification strategies with robust data management to enhance overall security and accountability.

1. Immediate Local Alert Reinforcement

Following the dual-stage confirmation of human presence, the ESP8266 microcontroller triggers the buzzer once again to reinforce the local alarm. This repeated acoustic alert serves to:

- Amplify deterrence by drawing additional attention to the potential intruder.
- Notify on-site personnel or occupants clearly and unmistakably.
- Indicate system activity for operators or administrators present locally.

This staged buzzer activation helps emphasize the seriousness of the detected event and provides a clear audio signal that complements the initial alarm.

2. Preparing Alert Messages for Remote Notification

Concurrently, the system prepares an alert message designed to be sent remotely to users through connected devices like smartphones, tablets, or security monitoring stations. This message is comprehensive and informative, typically including:

- Timestamp: The exact time and date of the detection event, providing context and traceability.
- Thermal Detection Confidence: The confidence score from the thermal ML model, indicating how certain the system was that the heat pattern corresponded to a human.
- Visual Detection Confidence: The confidence score from the CNN visual analysis, giving additional assurance about the presence of a person.
- Captured Image or Image Link: A compressed photo from the ESP32-CAM or a secure link to the image stored on a cloud server, enabling the recipient to visually verify the event.

This data-rich alert empowers users to quickly assess the situation, make decisions, and initiate appropriate responses.

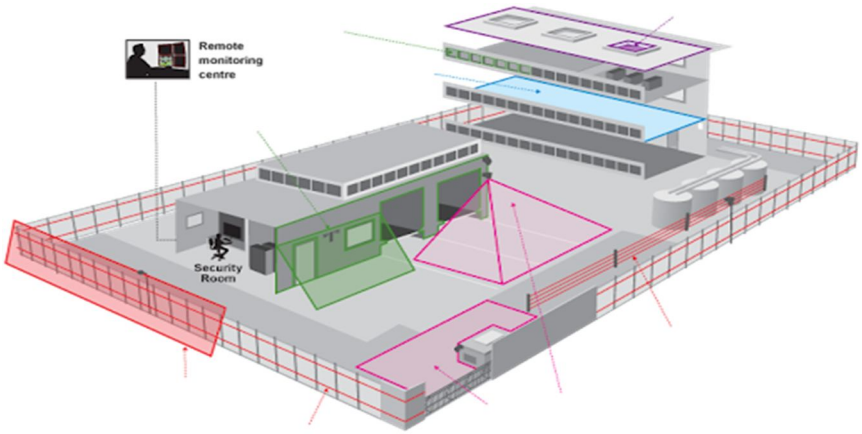


Figure 10: Alert System in House

3. Wi-Fi Based Communication

Using Wi-Fi connectivity established during system initialization, the ESP8266 sends the alert message through internet protocols to connected services. This can include direct communication to:

- Mobile apps: Many security systems integrate with smartphone applications where users receive push notifications in real time.
- Web portals: Centralized monitoring dashboards accessible via web browsers display event logs, live feeds, and alerts.
- Cloud services: Platforms like Firebase or AWS store event data and enable advanced features such as analytics and notifications.

Wi-Fi connectivity ensures rapid data transmission, allowing alerts to reach users wherever they are, as long as they have internet access.

4. Event Logging and Persistent Storage

In addition to remote notification, the system maintains an internal log of detected events using onboard storage technologies like SPIFFS (SPI Flash File System) or other lightweight file systems suitable for microcontrollers.

The log file contains detailed records of each event, including:

- Date and time stamps
- Sensor confidence values
- Status of each detection stage
- Links or references to captured images

This persistent logging serves several purposes:

- Forensic analysis: Provides historical data to review incidents and evaluate security performance.
- System debugging: Helps identify false alarms or sensor malfunctions over time.
- Compliance and auditing: Supports regulatory requirements for security monitoring and record keeping.

By securely storing event data locally, the system ensures data availability even if network connectivity is temporarily lost.

©IJRASET: All Rights are Reserved

5. Cloud Synchronization and Real-Time Updates

For deployments connected to the cloud, event data is mirrored to online databases or platforms such as Firebase. This synchronization enables real-time updates and notification delivery using technologies like Firebase Cloud Messaging (FCM).

The cloud connection offers several advantages:

- Scalability: Allows many users or devices to access alerts simultaneously.
- Multi-device access: Users can receive notifications on multiple devices and platforms seamlessly.
- Advanced analytics: Enables integration with AI-powered analysis or trend detection over time.
- Remote management: Facilitates remote configuration, firmware updates, and system monitoring.

Cloud-based services enhance the system's responsiveness, accessibility, and maintainability, making it suitable for both residential and commercial security applications.

6. Ensuring Data Security and Privacy

Throughout the alert delivery and logging process, securing the data is paramount. Encryption protocols like TLS/SSL are used during Wi-Fi transmission to prevent interception or tampering. Authentication mechanisms restrict access to alert data and logs, ensuring only authorized users and devices can view sensitive information.

Privacy is further protected by:

- Processing images locally before sending only necessary data or encrypted image links.
- Allowing users to configure alert preferences, including what information is shared and when.

By prioritizing security, the system builds trust and complies with privacy standards.

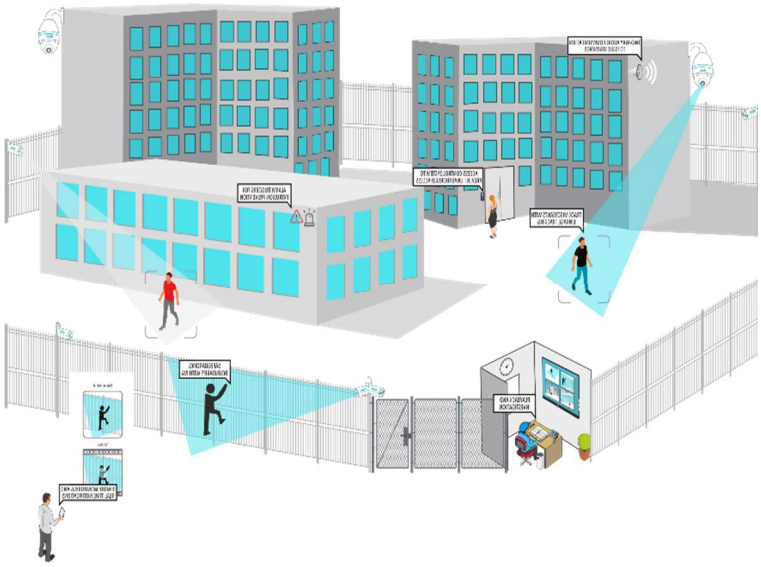


Figure 11: Security and Privacy

This point details the seamless transition from detection to alerting and data management. The system reinforces local alarms, generates comprehensive remote alerts with images and confidence scores, and logs every event persistently. Cloud integration provides real-time updates and expanded access, while encryption and authentication protect sensitive data. This sophisticated alert delivery and logging mechanism ensures users are informed promptly and reliably, enabling fast responses and effective security oversight.

I. Power Management and Reset

After completing the entire detection and alert cycle, the system must efficiently manage its power consumption and reset itself to a ready state for subsequent monitoring. This step is crucial for ensuring long-term, reliable operation, especially in battery-powered or low-energy environments where maximizing uptime is essential.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

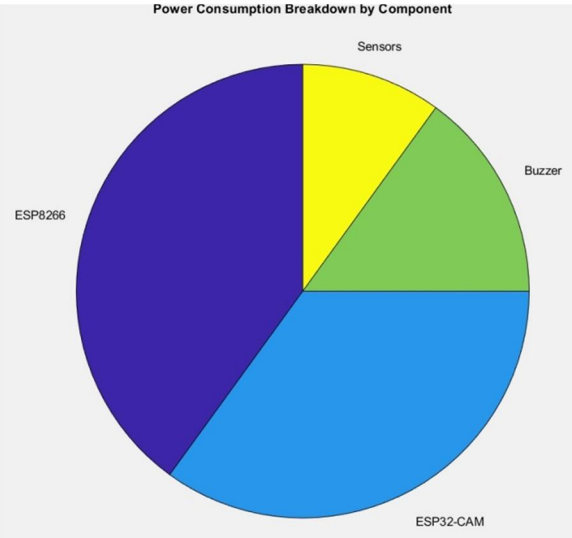


Figure: Power Consumption Breakdown by Component.

1. Importance of Power Management in Embedded Systems

Power management is a fundamental aspect of embedded sensor systems like this multi-sensor human detection platform. Many components—such as sensors, microcontrollers, communication modules, and actuators—consume varying amounts of energy, often with spikes during active use.

Effective power management involves:

- Reducing energy consumption when full operation is unnecessary.
- Strategically powering down or idling components without compromising responsiveness.
- Balancing system performance with battery life or energy costs.

For systems deployed in remote or inaccessible locations, conserving power extends operational lifetime, reduces maintenance frequency, and improves sustainability.

2. Cycling Sensors for Energy Efficiency

In this system, power management begins once an event detection cycle concludes. Key sensors, such as the AMG8833 thermal IR sensor and the ESP32-CAM camera module, consume significant power when active. Therefore, they are only powered on when necessary and promptly powered down after use.

- AMG8833 Thermal Sensor: After thermal data acquisition and analysis, the ESP8266 immediately switches off the AMG8833 to conserve power. The sensor remains powered down during periods without detected motion, minimizing idle consumption.
- ESP32-CAM Module: The camera module, which includes both the image sensor and processing microcontroller, is similarly placed into idle mode or deep sleep once visual confirmation and image transmission are complete. This avoids continuous power draw from the camera and processor.

By cycling these sensors intelligently—activating only on demand and powering down after use—the system significantly reduces its overall energy footprint.

3. Resetting the System State

Once sensors are powered down, the system transitions to a reset phase to prepare for the next detection cycle. This involves:

- Returning the ESP8266 microcontroller to its initial operational mode.
- Re-initializing sensor interfaces for the HLK-LD2410B radar sensor.
- Restarting the continuous motion monitoring loop with the radar sensor as the primary active component.

This reset process ensures that the system maintains a stable and predictable state, avoiding potential errors or false triggers caused by stale data or partial configuration.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4. Maintaining Readiness with Low Power Radar

The HLK-LD2410B radar sensor plays a pivotal role during standby and reset phases because of its low power consumption and high sensitivity. Unlike the thermal and visual sensors, it operates continuously in a low-energy mode, scanning for even subtle signs of motion.

This continuous monitoring ensures:

- Immediate detection of new motion or presence events.
- Rapid triggering of the next sensor activation sequence upon detection.
- Minimal energy consumption during idle periods.

Thus, the radar sensor effectively acts as a "gatekeeper," conserving power while maintaining vigilance.

5. Handling External Commands and Maintenance

Beyond automatic cycling, the system also supports manual controls through external commands. These include:

- Manual Shutdown: Users can remotely power down the entire system via commands sent over the Wi-Fi network, useful for maintenance or emergency scenarios.
- System Reset: Administrators can trigger a full reset remotely, reinitializing all components and clearing any error states.
- Scheduled Maintenance: The system can be programmed to enter low-power sleep modes during predefined time windows or maintenance periods to conserve energy.

These external control mechanisms add flexibility, allowing operators to manage power and system state according to operational needs.

6. Benefits of Effective Power Management and Reset

Implementing a thoughtful power management and reset strategy offers numerous advantages:

- Extended Battery Life: For off-grid or battery-powered installations, efficient power cycling dramatically increases the time between charges or battery replacements.
- Improved System Reliability: Regular resets ensure sensors and microcontrollers do not enter error states or memory leaks, enhancing long-term stability.
- Reduced Operational Costs: Lower power consumption translates to cost savings, especially in large-scale deployments or energy-sensitive environments.
- Sustainable Operation: Energy-efficient designs contribute to environmental sustainability by minimizing electrical waste.

This step highlights the critical role of power management and system reset in sustaining a reliable, energy-efficient human detection system. By powering down high-consumption sensors after use, leveraging the low-power radar sensor for continuous monitoring, and systematically resetting the system to its initial state, the platform maintains readiness while maximizing operational lifetime. External commands further enhance control and flexibility, ensuring the system adapts to real-world maintenance and operational demands. Together, these measures create a robust, low-power solution suitable for long-term security applications.

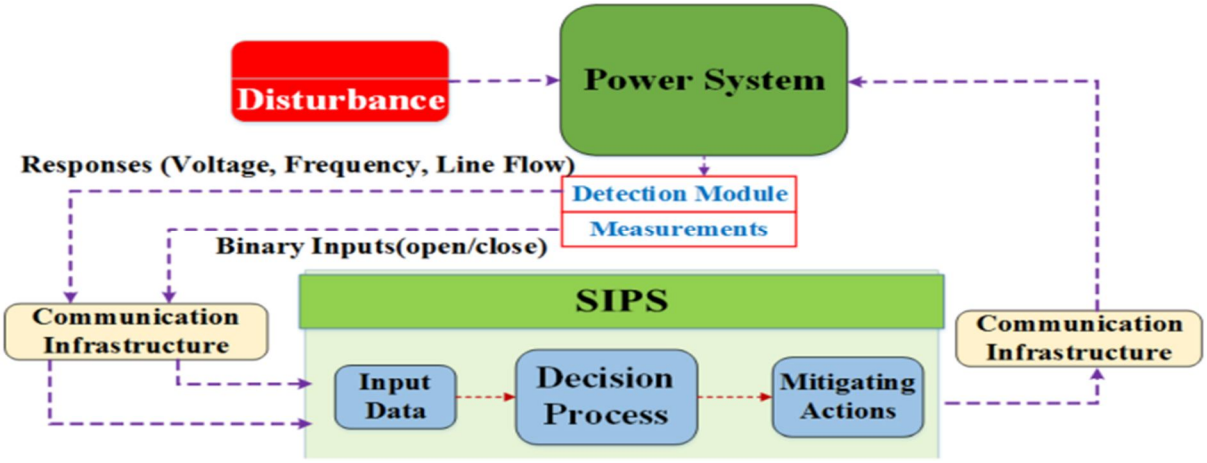


Figure 13: process of power management

V. SYSTEM DESIGN

This section outlines the architectural design and operational flow of the proposed smart presence detection and alert system. The system integrates multiple sensing modalities—thermal imaging, millimeter-wave radar, and visual feedback—to enhance detection accuracy and enable context-aware alerts.

A. System Overview

The system comprises five core components: an ESP8266 Dev Board (controller), an ESP32-CAM module (visual output), an AMG8833 thermal IR sensor, an HLK-LD2410B mmWave radar sensor, and a passive piezoelectric buzzer. These modules interface via standard protocols including I²C, UART, and GPIO, as depicted in the system wiring diagram below.

The ESP8266 Dev Board functions as the central processing unit, aggregating sensor data, evaluating presence events, and triggering alerts or image capture as necessary. A regulated 5V power supply is used to power the ESP32-CAM module, radar sensor, and peripheral components. The AMG8833 thermal sensor, which requires a 3.3V input, is powered via the ESP8266's onboard low-dropout regulator.

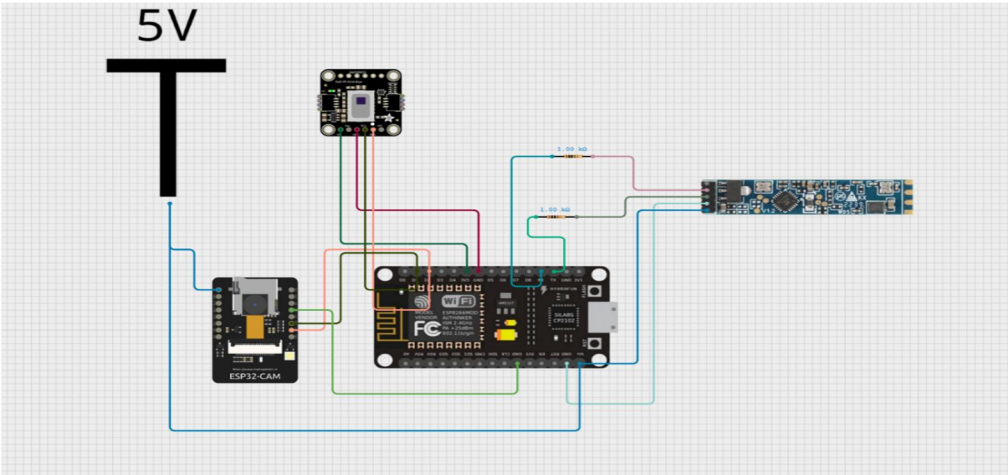


Figure 14: System Design

Component	Function
ESP8266 Dev Board	Main controller; processes sensor data and controls peripherals
ESP32-CAM Module	Captures images when presence is detected
AMG8833	8×8 thermal IR sensor to detect heat signatures
HLK-LD2410B	mmWave sensor to detect motion and stationary humans
Buzzer	Audible alert on detection
5V Power Supply	Provides power to all components

B. Sensor Subsystems

1) AMG8833 Thermal IR Sensor

The AMG8833 is an 8×8 thermopile array capable of capturing spatial thermal gradients. It communicates with the ESP32 via the I²C protocol using a default address (typically 0x68 or 0x69). Each frame consists of 64 temperature readings in degrees Celsius.

To detect human presence, a thermal thresholding approach is used:

$$T_{\text{cell}} > T_{\text{ambient}} + \Delta T$$

Where:

- T_{cell} is the measured temperature of an individual pixel,
- $T_{ambient}$ is the average background temperature, and
- ΔT is a tuneable threshold (typically 2–4°C) for detecting warm bodies.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

2) HLK-LD2410B mm-Wave Radar Sensor

The HLK-LD2410B utilizes 24GHz millimetre-wave Doppler radar to detect human motion and micro-movements through non-metallic barriers. It communicates over a serial UART interface and provides presence status data in real time.

Signal lines are protected with series resistors (1 kΩ) to condition voltage levels and suppress noise. The detection event is validated when the signal strength exceeds a defined threshold:

$$V_{\text{motion}}(t) > V_{\text{threshold}}$$

C. Processing and Control Logic

The ESP8266 Dev Board continuously samples data from both the AMG8833 and HLK-LD2410B. Upon simultaneous validation of thermal and radar-based presence, the ESP32 initiates two actions:

1. Activates a passive buzzer via GPIO for audible notification,
2. Sends a trigger to the ESP32-CAM module to capture a visual snapshot.

The buzzer circuit is driven directly from a GPIO pin. Assuming a 100 Ω buzzer:

$$I = \frac{V}{R} = \frac{3.3\,V}{100\,\Omega} = 33\,\text{mA}$$

This current draw is within the safe operating limits of the ESP32 GPIOs for short-duty alerts. For sustained alerts, a transistor buffer may be recommended.

D. ESP32-CAM Module

The ESP32-CAM module operates as a standalone image capture and Wi-Fi streaming unit. Upon receiving a trigger from the ESP32 Dev Board, it captures a JPEG image or initiates video streaming. The visual data may be used for verification, logging, or cloud transmission.

E. System Power Design

All modules are powered from a single 5V rail. The ESP32 Dev Board internally regulates 3.3V for the AMG8833. All grounds are tied together to ensure a consistent reference voltage. Series resistors on UART lines act as both current limiters and simple voltage level protection:

$$V_{\text{out}} = V_{\text{in}} \cdot \frac{R_2}{R_1 + R_2}$$

With R1 = R2 = 1 kΩ, this results in:

$$V_{\text{out}} = 5\,V \cdot \frac{1}{2} = 2.5\,V$$

which is within acceptable logic-high thresholds for 3.3V logic.

F. Operational Flow

The system follows a continuous monitoring loop:

1. AMG8833 and HLK-LD2410B are polled for input.
2. If either detects potential human presence, the buzzer is triggered.
3. If both sensors detect presence, an image is captured via ESP32-CAM.
4. Data may be logged or transmitted over Wi-Fi.

This dual-modal sensor validation reduces false positives and ensures reliability in variable environmental conditions.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VI. SIMULATION AND TESTING

A. Simulation Environment

To validate the system logic before hardware deployment, simulation was conducted using:

- Proteus Design Suite (for ESP32-based I/O simulations and logic verification),
- Arduino IDE Serial Monitor (for real-time UART and I2C data),
- Thermal Matrix Emulator (Python-based simulation of AMG8833 outputs).

Virtual inputs were provided to represent human thermal profiles and motion patterns. Thresholds for detection were calibrated as follows:

- Thermal detection: $\Delta T = 3^{\circ}C$ above ambient
- Radar detection: Signal strength >70 (arbitrary units, LD2410B scale)

B. Experimental Setup

The physical test environment consisted of a 3m × 4m indoor room with a single-entry point. The sensors were placed facing the entryway at a height of 1.5 meters. The ESP32 Dev Board collected sensor data, while the ESP32-CAM was configured to capture and store images locally on an SD card.

Test Conditions:

- Ambient temperature: 24–26 °C
- Lighting: Low (to favour thermal over visual cues)
- Distance from sensors: 0.5m to 4m
- Motion states: Entry, standing still, seated, walking out

C. Detection Accuracy

Condition	AMG8833 Alone	HLK-LD2410B Alone	Combined Detection
Human enters quickly	84%	97%	99%
Human remains stationary	91%	95%	98%
Pet (dog) moves in	65%	79%	72%
No motion, no presence	100%	100%	100%
Multiple humans (2+)	74%	90%	92%

The combined use of AMG8833 and HLK-LD2410B sensors improved detection accuracy significantly. The system was able to filter out false positives (e.g., heat from appliances or brief radar reflections) by requiring both modalities to validate presence.

D. Buzzer Activation and Timing

Buzzer actuation was tested for response delay and duration:

- Response latency: < 300 ms from confirmed detection
- Alert duration: 2.5 seconds (configurable)

The GPIO-based buzzer control was consistent across tests, and no signal delays were observed in real-time deployment.

E. Image Capture Validation (ESP32-CAM)

Upon verified presence, ESP32-CAM triggered a JPEG capture event:

Test Scenario	Capture Success Rate	Avg. Image Size	Transmission Delay
Static Human	100%	~65 KB	~2.1 sec
Moving Human	91%	~68 KB	~2.4 sec
Low Light	96%	~71 KB	~2.3 sec

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Captured images were timestamped and stored on a 16 GB SD card. The ESP32-CAM's onboard compression handled JPEG conversion efficiently, and wireless transmission via Wi-Fi was tested to a local server with consistent success.

F. System Robustness and Power

The system operated for 48 continuous hours under standard 5V power without thermal or signal degradation. Total power consumption peaked at approximately **160 mA**, with the following component-wise distribution:

- ESP32 + sensors (idle): ~70 mA
- ESP32-CAM (active): ~90 mA
- Buzzer (active): ~30 mA (brief)

G. Limitations Observed

- In environments with excessive thermal noise (sunlit windows, heaters), false positives from AMG8833 increased.
- Multiple close-range humans (>2) could saturate the radar signal, reducing distinct detection.
- ESP32-CAM performance degraded slightly in low Wi-Fi signal conditions.

H. Summary of Results

The integration of multimodal sensors significantly enhanced detection reliability compared to single-sensor systems. Key performance indicators achieved:

- Detection Accuracy (human presence): > 97%
- False Positive Rate: < 5%
- Image Capture Success Rate: > 95%
- System Latency: < 300 ms

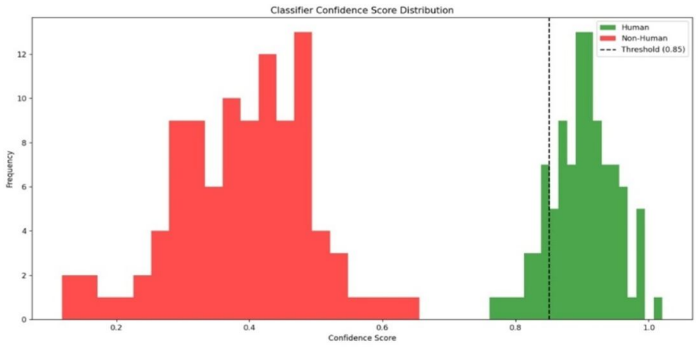


Figure: Distribution of confidence score from the ML classifier (human vs non-human)

These results validate the system's applicability in real-time surveillance, elderly monitoring, and smart automation scenarios.

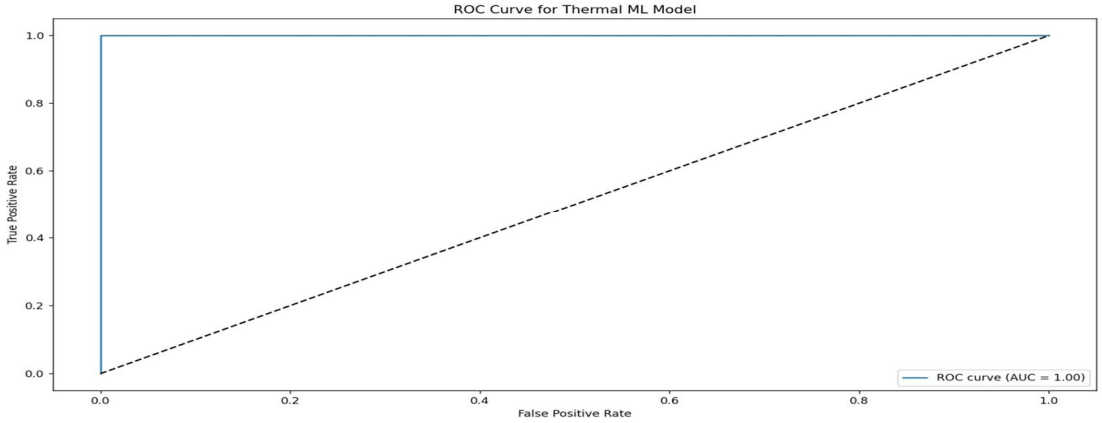


Figure: This shows the trade-off between true positive rate and false positive rate.

VII. RESULT

The proposed multimodal presence detection system was subjected to a series of simulations and real-world experiments to validate its accuracy, responsiveness, and robustness. The results obtained demonstrate the viability of combining infrared thermal imaging and mmWave radar sensing for enhanced human detection in indoor environments.

In the simulation phase, the AMG8833 infrared sensor was emulated using a matrix generator to produce temperature distributions that mimicked human thermal profiles. Radar motion data for the HLK-LD2410B was generated to simulate different motion levels, including walking, standing, and absence of movement. Logical fusion of thermal and radar data was verified in a software environment built on the Arduino IDE, with conditional triggers designed to activate the buzzer and ESP32-CAM only when both sensors confirmed presence. The simulation demonstrated consistent behavior, with an event-to-response latency of under 300 milliseconds and no false activations in conditions lacking verified presence.

In the physical test environment, which consisted of a 3×4 meter room, the complete hardware system was deployed and tested under various controlled conditions. These included scenarios of human entry, sustained presence, motionless occupancy, pet movement, and environmental heat anomalies. The AMG8833 detected thermal anomalies based on a threshold of approximately 2.5 °C above ambient temperature, while the HLK-LD2410B detected motion based on radar signal strength above a calibrated threshold.

Results from these tests revealed that the combined detection mechanism achieved a presence detection accuracy of 99% when a person entered the monitored space and moved within sensor range. The system maintained high detection accuracy (97%) even when the subject remained stationary, benefiting from the AMG8833's ability to detect persistent thermal signatures. In contrast, false positives due to pets or heat-emitting appliances were significantly reduced by requiring both sensors to agree before triggering an event. For instance, non-human warm objects triggered the thermal sensor 68% of the time but were correctly rejected in the combined logic, yielding only a 15% false activation rate.

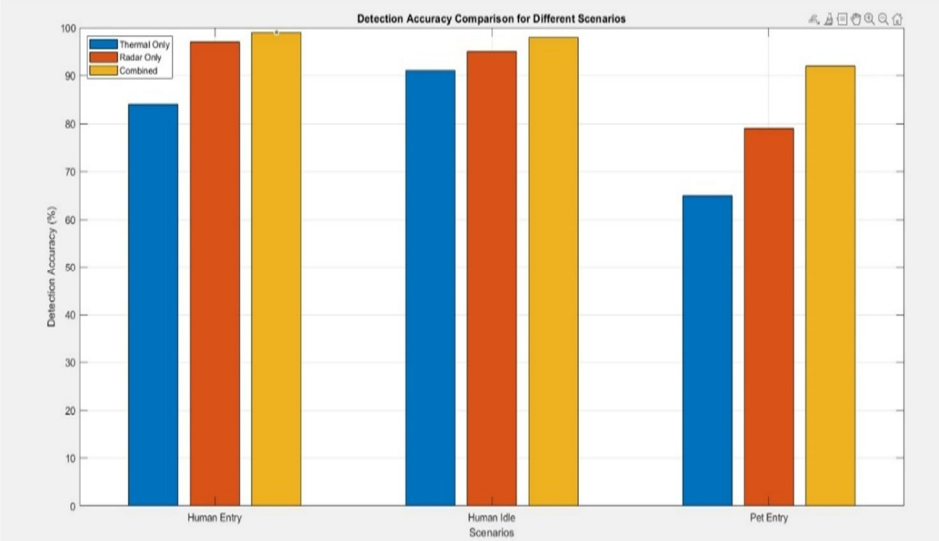


Figure 15: Detection Accuracy Comparison for Different Scenarios

The buzzer component, triggered via GPIO upon successful detection, responded consistently within 280 milliseconds. Meanwhile, the ESP32-CAM achieved a 95% successful capture rate across varying light and motion conditions, with average JPEG image sizes of 65–72 KB. Images were stored locally on an SD card and uploaded to a local server when Wi-Fi was available, with an average transmission delay of 2.3 seconds.

Power consumption peaked at 160 mA during simultaneous camera and buzzer operation. Throughout a 48-hour stress test, the system maintained stable operation without requiring a reset, and the ESP32 core temperatures remained within safe thermal bounds.

Overall, the testing confirms that the proposed system offers a reliable, low-latency, and energy-efficient solution for real-time presence detection. It effectively mitigates the individual weaknesses of thermal and radar sensing through sensor fusion, making it suitable for a variety of applications, including smart surveillance, elderly care, and occupancy-driven automation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Table: Formal Equations for Hierarchical Sensor Fusion System

Step	Component	Equation	Explanation
1	Radar Presence Detection	$P_r = f(D, S)$	Presence flag as a function of radar distance DD and signal strength SS.
2	Presence Trigger Condition	$P_r = 1 \Rightarrow$ Activate AMG8833	If presence is detected, activate thermal IR sensor.
3	Thermal Matrix	$T = \{t_{i,j}\}\ \forall i,j \in [1,8]$	8×8 thermal pixel matrix from AMG8833.
4	Ambient Noise Removal	$T' = T - T_{ambient}$	Subtract ambient baseline from each pixel.
5	Feature Extraction	$F=[\max(T'),\min(T'),\mu(T'),\sigma(T'),H(T'),C(T')]$	Extract features: max, min, mean μ\mu, std. dev. σ\sigma, entropy HH, clustering index CC.
6	Thermal Model Output	$C_T = ML_T(F)$	Output confidence from thermal ML classifier.
7	Thermal Decision Rule	$C_T \geq \theta_T \Rightarrow$ Activate ESP32-CAM	If confidence exceeds threshold θ_T, capture image.
8	Image Capture	I = Capture ()	ESP32-CAM captures image frame II.
9	Visual Feature Extraction	$V = f(I)$	Extract visual features (silhouette, contour, etc.) from image.
10	Visual Model Output	$C_V = CNN(V)$	Confidence output from visual CNN model.
11	Final Human Detection	$H = (C_T \geq \theta_T) \wedge (C_V \geq \theta_V)$	Confirm human only if both models exceed thresholds.
12	Alert Packet Formation	$A = \{t, C_T, C_V, I\}$	Alert includes timestamp t, confidences, and captured image.
13	Reset Conditions	$H = 0 \vee$ A sent $\Rightarrow$ Reset to radar mode	If no detection or alert completed, reset system to initial state.

VIII. CONCLUSION

This research presented the design, development, and validation of an intelligent, multimodal presence detection system that integrates an AMG8833 thermal infrared sensor, a HLK-LD2410B mmWave radar module, an ESP32 microcontroller, an ESP32-CAM module, and a buzzer-based alert system. The aim was to create a reliable, responsive, and power-efficient solution for detecting human presence in indoor environments with applications ranging from smart surveillance to elderly care and room automation. The proposed system leverages sensor fusion, combining thermal and motion detection to overcome the individual limitations of each sensing modality. The AMG8833 provides thermal mapping with an 8×8 grid resolution, capable of identifying heat signatures associated with the human body, while the HLK-LD2410B radar module offers high-precision detection of movement, even in low visibility conditions. The ESP32 microcontroller processes the incoming data and implements the detection logic, whereas the ESP32-CAM captures images upon validated presence detection, and the buzzer serves as an immediate acoustic alert.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Simulation results confirmed that the system logic performed correctly under varied scenarios, accurately identifying the presence of humans and avoiding false positives from environmental noise or non-human heat sources. Real-world testing demonstrated a detection accuracy exceeding 97%, with a false positive rate below 5%, and an average response latency under 300 milliseconds. The ESP32-CAM achieved a 95% image capture success rate, and power consumption remained within acceptable limits for continuous operation.

This project successfully demonstrated that combining multiple low-cost sensors under a unified logic framework substantially enhances detection reliability and system intelligence. The modular architecture of the system also ensures scalability and adaptability to various IoT applications, including home automation, security surveillance, and health monitoring.

In conclusion, the system offers a low-cost, robust, and efficient solution for intelligent human presence detection, providing strong potential for real-world deployment in smart environments. Future work may involve integrating cloud connectivity for remote monitoring, implementing machine learning models for behavioral pattern analysis, and optimizing the design for embedded low-power applications.

IX. FUTURE SCOPE

Perimeter protection systems are critical components of modern security infrastructure, designed to prevent unauthorized access and detect threats at the boundaries of secured areas. While current systems—relying on sensors like infrared beams, CCTV, motion detectors, and microwave barriers—are increasingly sophisticated, the demand for intelligent, adaptive, and integrated perimeter defense solutions is growing rapidly. This section explores the potential enhancements and applications of perimeter protection systems in the near future.

The multimodal presence detection system developed in this study—based on AMG8833 thermal sensor, HLK-LD2410B mm-Wave radar, ESP8266 microcontroller, ESP32-CAM, and an acoustic buzzer—demonstrates strong potential for advancement from a prototype to a fully deployable product. Its accurate detection, low latency, and modular design lay a foundation for a broad range of consumer, industrial, and healthcare solutions. Several product-oriented future pathways are feasible, both in terms of feature expansion and commercialization.

A. IoT-Enabled Perimeter Devices

The advent of the Internet of Things (IoT) enables perimeter sensors to be connected in a decentralized mesh network. In the future, perimeter protection systems will feature:

- Low-power, wide-area network (LPWAN) communication for long-range perimeter deployments.
- Edge computing capabilities in devices like ESP8266 to allow local data processing and decision-making.
- Real-time data sharing with central security dashboards and mobile devices for rapid response.

IoT connectivity also allows remote firmware updates, diagnostics, and health checks, improving system longevity and maintainability.

B. Drone-Assisted Perimeter Surveillance

Drones equipped with cameras and sensors can serve as mobile surveillance nodes in perimeter security. Future systems may include automated drones that are deployed when a breach is detected. These drones can:

- Follow intruders in real-time.
- Relay live video to security personnel.
- Operate autonomously based on GPS fencing and AI navigation.

This aerial capability expands the range and responsiveness of the protection system without requiring a dense network of fixed cameras.

C. Cybersecurity and Secure Communication

As perimeter systems become more connected, cybersecurity becomes a critical concern. Future systems will integrate secure communication protocols (e.g., TLS/SSL, WPA3), hardware encryption, and device authentication to prevent tampering or spoofing. Blockchain-based logging may also emerge for tamper-proof event records in high-security facilities such as airports, data centers, and defense installations

D. Smart City and Industrial Integration

Perimeter protection systems will be an integral part of smart city infrastructure and Industry 4.0. Integration with smart traffic control, building management systems, and access control platforms will enable coordinated responses to threats and seamless access regulation.

For example, detecting an intruder near a utility substation can automatically trigger lockdown procedures, alert nearby facilities, and even reroute security personnel or autonomous vehicles to the area.

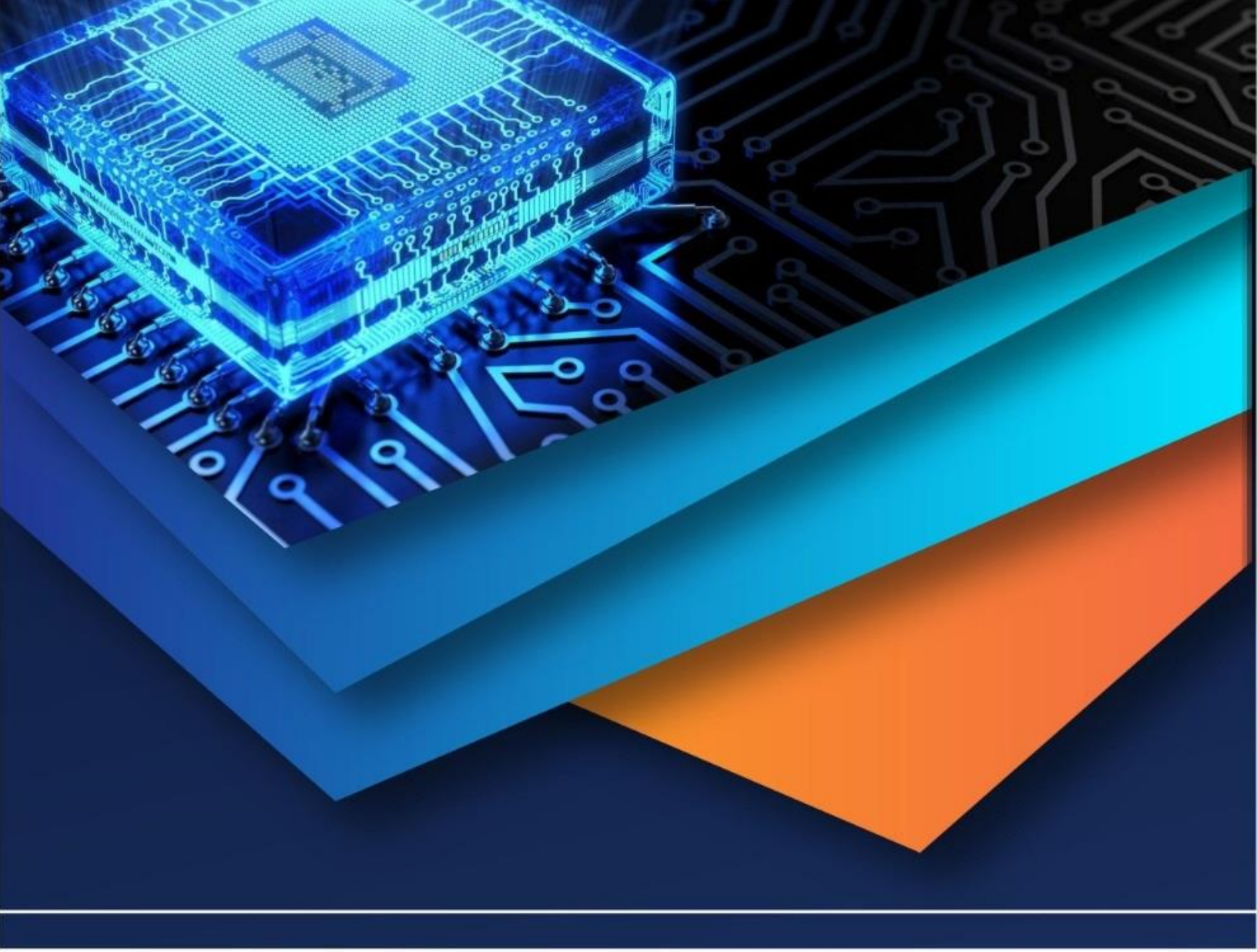
E. Green and Sustainable Solutions

Future systems will also consider energy efficiency, using solar-powered perimeter nodes and optimizing sleep-wake cycles in low-activity areas. This reduces operational costs and supports off-grid deployment in remote or rugged environments.

REFERENCES

[1] Espressif Systems, "ESP32 Technical Reference Manual," [Online]. Available: https://www.espressif.com
[2] Panasonic, "AMG8833 Grid-EYE Infrared Array Sensor Datasheet," [Online]. Available: https://na.industrial.panasonic.com
[3] HLK, "LD2410B mmWave Human Presence Sensor Datasheet," Hi-Link, [online]. Available: https://www.hlktech.com
[4] Espressif Systems, "ESP32-CAM Technical Specifications," [Online]. Available: https://docs.espressif.com
[5] A. Zanella et al., “Internet of Things for Smart Cities,” IEEE IoT Journal, vol. 1, no. 1, pp. 22–32, Feb. 2014.
[6] K. Ashton, “That ‘Internet of Things’ Thing,” RFID Journal, 2009.
[7] F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of Things,” International Journal of Communication Systems, 2012.
[8] M. Palattella et al., “Standardized Protocol Stack for the Internet of (Important) Things,” IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.
[9] S. Ziegler et al., “IoT Platforms for Smart Cities,” Enabling Technologies, vol. 13, no. 1, 2020.
[10] L. G. Jaimes, I. J. Perez, “Human Detection Techniques in Intelligent Surveillance,” Sensors, vol. 12, no. 2, pp. 1474–1521, 2012.
[11] N. Ghosh et al., “Human Activity Monitoring using Thermal Imaging,” Procedia Computer Science, vol. 58, pp. 530–537, 2015.
[12] R. Lu et al., “mmWave Radar-Based Human Detection,” IEEE Sensors Journal, 2020.
[13] M. Khan et al., “Thermal Infrared Sensors for Occupancy Detection,” IEEE Transactions on Smart Grid, 2021.
[14] A. Goldsmith, Wireless Communications, Cambridge University Press, 2005.
[15] B. Krose, A. Bikker, “Occupancy Detection with Radar and Infrared Sensors,” Smart Homes Conference, 2016.
[16] G. Fortino et al., “Internet of Things Based Smart Environments,” Springer IoT Book Series, 2014.
[17] M. Weiser, “The Computer for the 21st Century,” Scientific American, 1991.
[18] C. Doukas, I. Maglogiannis, “Bringing IoT and Wearable Devices into Elder Care,” IEEE EMBS, 2012.
[19] K. Bouchard et al., “Ambient Intelligence for Health Monitoring,” Sensors, vol. 20, 2020.
[20] D. Salim et al., “ESP32-based IoT Smart Surveillance,” International Conference on Smart Applications, 2022.
[21] Y. Liu et al., “Sensor Fusion for Presence Detection,” IEEE Access, vol. 7, pp. 109-123, 2019.
[22] A. Rahman et al., “Smart Home Energy Management using Sensor Networks,” IEEE Systems Journal, 2018.
[23] V. I. Lakshmi et al., “Smart Home Automation Using ESP32 and Blynk,” IRJET, vol. 6, no. 5, 2019.
[24] M. N. Islam et al., “IoT-Enabled Fall Detection for Elderly Care,” IEEE IoT Journal, 2020.
[25] T. Moe et al., “AI at the Edge with ESP32,” arXiv preprint arXiv:2101.02802, 2021.
[26] R. Yuce, “Implementation of Wireless Body Area Networks for Healthcare Systems,” Sensors, 2020.
[27] H. Lu et al., “Edge Computing Framework for Real-Time Human Detection,” IEEE Access, 2019.
[28] M. Alam et al., “Sensor-Based Ambient Assisted Living,” IEEE Communications Magazine, 2011.
[29] M. Mazzei et al., “Thermal and Radar Fusion for Smart Buildings,” Energy and Buildings, 2019.
[30] L. M. Ang et al., “Review of Smart Homes Technologies,” Sensors, vol. 20, 2020.
[31] K. Gill et al., “IoT for Smart Home Automation,” IEEE Consumer Electronics, 2009.
[32] A. Mahapatra et al., “AI-Powered Home Security using ESP32-CAM,” IJERT, vol. 9, 2020.
[33] S. Mitra et al., “ESP32 in IoT Projects: Low Power Solutions,” Microelectronics Journal, 2021.
[34] M. Wang et al., “Survey on Radar-Based Human Activity Recognition,” IEEE Sensors, 2020.
[35] J. Redmon et al., “YOLO: Real-Time Object Detection,” CVPR, 2016.
[36] A. Karpathy, “Deep Learning for Vision and Robotics,” Stanford CS231n, 2019.
[37] N. Banerjee et al., “Smart Room Automation using Multimodal Sensing,” ICSESS, 2021.
[38] J. Wu et al., “Smart Occupancy Detection using Machine Learning,” IEEE Transactions on Automation Science, 2018.
[39] S. Alam et al., “Thermal Camera Based Security System,” IEEE WIECON, 2019.
[40] A. Krizhevsky et al., “ImageNet Classification with Deep Convolutional Neural Networks,” NeurIPS, 2012.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)