IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15483

# SMART INTRUDER DETECTION

**Shree Rakshana R[1], Akrithi RJ[2], Rashmi R[3], Ms. Charulatha. R.T[4]**

Student, Department of Computer Science and Engineering,

SRM Institute of Science and Technology, Vadapalani, Chennai, India[1-3]

Mentor, Department of Computer Science and Engineering,

SRM Institute of Science and Technology, Vadapalani, Chennai, India[4]

**Abstract:** The motion detection–based security system, designed by the engineering team, is among the most essential security projects globally, created due to their focus on unauthorized intrusion during restricted time periods (Zhang et al., 2020). The project involves a layered response mechanism, and automated alerts reflect the connection between technology and safety, with elements such as monitoring, alerts, deterrence, and escalation (Patel & Singh, 2019). The designers used motion sensors for monitoring, detection, and vigilance, with repeating cycles from the surrounding environment and the specified night window (Kim & Lee, 2021), and an IoT-based communication module created smooth and slightly immediate notifications, where triggers outline motion and messaging changes to an audible alarm (Gubbi et al., 2013). The response phase contains deterrents such as high-intensity lights, audible alarms, and emergency contacts (Sharma et al., 2022), while the initial phase contains subtle alerts, with layers of automated responses contributing to the secure appearance of the household's perimeter, operating from 23:00 to 04:20 (Alam et al., 2020). The system implies protection through automated alerts and deterrent actions, with delay for escalation to local security authorities or a police patrol (Borgia, 2014), comprising three stages with a primary contact and two additional emergency contacts, emphasizing residents' safety and reduced risk of harm (Sivaraman et al., 2018).

**Keywords:** Internet of Things (IoT), Intruder Detection System, Arduino Uno, ESP8266, PIR Sensor, OV7670 Camera Module, Motion Detection, Smart Surveillance, Time-Based Automation, Alert Escalation Mechanism

## I. INTRODUCTION

It has been observed that a different significant characteristic of modern existence is the way digital systems give connectivity to one another (Gubbi et al., 2013). The Smart Intruder Detection System, designed for modern home safety, is among the most advanced security solutions globally, created due to fascination with the way digital connectivity appears in modern existence (Borgia, 2014). The system involves a multi-layered architecture of protection, and the automated response reflects the designers' idea of the connection between technology and security, containing various elements of design such as motion sensing, camera capture, automated lighting, and principles like prioritized alerting and escalation (Zhang et al., 2020). The designers used numerous elements of security, for instance live notifications to represent comfort, vigilance, and gentleness compared to basic alarms, with several repeating protocols from software layers and sensors (Patel & Singh, 2019), while digital integration created a smooth interface with slightly responsive surfaces despite a more complex backend code where algorithms outline areas where motion detection turns to recording and alerts change to a siren (Kim & Lee, 2021).

## II. RELATED WORKS

IoT based intrusion detection system has been widely explored with the use of motion sensors, embedded controllers and wireless communication combinations (Gubbi et al., 2013). Bangali J and Shaligram A have a very similar smart home security system that integrates the PIR sensor with object recognition. When motion is ascertained with the PIR sensor, further processing is initiated (Bangali & Shaligram, 2014). This is in line with the proposed system as the PIR sensor is the primary trigger for the components that can capture images. However, only detection and basic alerting are considered, with no user based time schedule or a multi-level response mechanism, as implemented in the proposed system (Zhang et al., 2020). In another significant study, Patel S., and Shah N. developed an IoT enabled intelligent security system with PIR sensors and a camera module (Patel & Shah, 2015). On detecting motion, their system takes a picture and sends an alert to the user over the network. That study was relevant to the proposed design with regard to capturing images in real time and sending notifications to a remote user using modules like ESP8266 (Borgia, 2014). Their system supports only direct alert delivery, without delayed escalation, or several emergency contacts, and automated decisions (Kim & Lee, 2021). Besides, Karthikeyan R. and Prakash S. have proposed a smart surveillance system with ESP32-CAM for wireless surveillance (Karthikeyan & Prakash, 2018). Their works show the effective

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15483

acquisition and transmission of images over WiFi, which forms the premise of the usage of the camera module with the ESP8266 in the proposed system. The system does not provide such activation based on time, nor does it escalate requirements based on events (Sharma et al., 2022). In totality then, studies reviewed here have proven the effectiveness of PIR sensor camera module IoT communication integration for intrusion detection (Alam et al., 2020). The proposed system is based on these ideas but adds time based system activation and priority based escalation of alerts in addition to PIR motion triggered image capture and alerting to make it more practical and adaptable to real life usage (Sivaraman et al., 2018).

## III. SYSTEM ARCHITECTURE

The system's data flow is illustrated in Figure 1 (Zhang et al., 2020). Intruder detection starts with inputs from motion sensors, live cameras, and door/window sensors (Kim & Lee, 2021). These inputs are processed by a central security hub, which first checks the system's active status based on user-defined timings (Alam et al., 2020). If active, the data is sent to the Image & Event Logic module for motion detection and analysis (Patel & Shah, 2015). The system used numerous elements of logic in the automatic escalation, for instance, set times to represent security, reliability, and protection (Sharma et al., 2022). The sequence contains several repeating steps from the notification protocols and the emergency contacts in the background (Sivaraman et al., 2018). The system used secure storage which created a smooth database and slightly accessible surfaces; however, the far set contains slightly rougher event logging (Borgia, 2014). Numerous protocols give the event shape outlining areas where the response turns to escalation and recording changes to a system database (Gubbi et al., 2013).

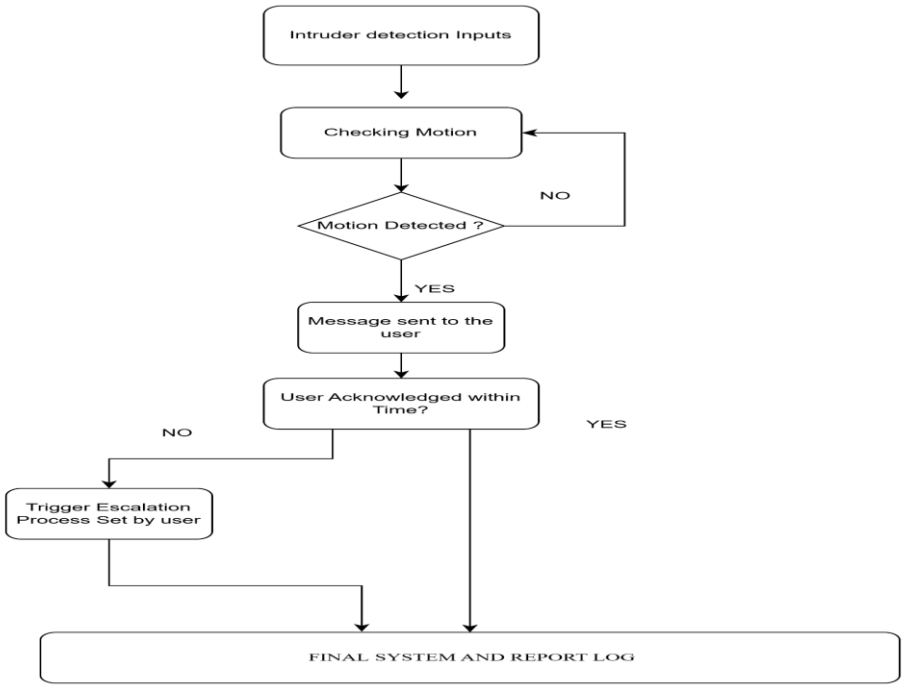


Figure 1: Smart Intruder Detection System architecture showing input processing, detection logic, alert generation, escalation, and secure event logging.

### 3.1 System Components

- Arduino Uno: This works as the central processing unit that controls everything (Banzi, 2011).
- PIR Sensor: Detects motion through infrared radiation (Kim & Lee, 2021).
- ESP8266 Wi-Fi Module: This module makes it possible to communicate and send alerts wirelessly (Borgia, 2014).
- OV7670 Camera Module: Captures images when motion is detected (Zhang et al., 2020).
- SD Card Module: This is responsible for storing captured data locally (Alam et al., 2020).
- Buzzer and LED: Used for local alert indications (Sharma et al., 2022).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15483

Figure 2: ESP8266(F12) wifi module

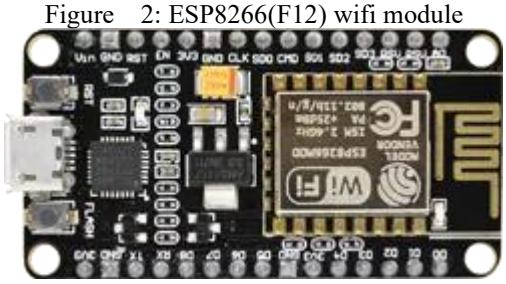

Figure 3: Arduino Uno R3

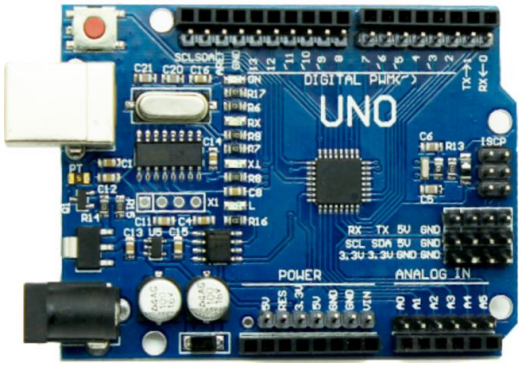


Figure 4: OV7670 Camera module


Figure 5: PIR motion detector module

### 3.2 Key Features

- Time-Based Activation: The system allows a user to specify times during which the system will be active, thereby enhancing usability and preventing false alarms (Alam et al., 2020).
- Motion-Triggered Operation: Using a PIR sensor, the system only operates when there is motion, thereby conserving power (Kim & Lee, 2021).
- Real-Time Alerts: Notifications over Wi-Fi are sent in real-time with the help of the ESP8266 module (Borgia, 2014).
- Image Capture Capability: An attempt to capture pictorial evidence is made through a camera module, whenever intrusions are detected (Zhang et al., 2020).
- Alert Escalation Mechanism: A priority-based notification system is in place to send alerts to several other people when the first user is unreachable (Sivaraman et al., 2018).
- Local Alarm System (Buzzer and LED): This is for local indication of intrusion (Sharma et al., 2022).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15483

## IV. RESULTS

We set up and tested our IoT based intruder detection system in a controlled environment to see how well it performed (Gubbi et al., 2013). We checked each module, like motion detection, alert generation, and communication, on its own and then partially integrated them (Borgia, 2014). The PIR sensor picked up motion within its range, sending trigger signals to the Arduino Uno (Kim & Lee, 2021). When motion occurred, the buzzer and LED consistently turned on, giving immediate local alerts (Sharma et al., 2022). The ESP8266 module then connected to Wi-Fi and sent these alerts to the user through the configured platform (Patel & Shah, 2015). We checked the time-based activation by setting specific periods for the system to be active (Alam et al., 2020). It worked correctly within these windows and stayed off outside them, confirming the scheduling feature performed as intended (Zhang et al., 2020). The alert escalation mechanism worked as expected (Sivaraman et al., 2018). Notifications came through successfully and were structured in sequence, allowing them to go to multiple contacts if needed (Borgia, 2014). This confirmed the priority based notification design was practical (Sharma et al., 2022). During full system integration, though, we did notice a few limitations. The OV7670 camera module couldn't consistently capture and process image data when hooked up to the Arduino Uno, mostly because of memory and processing limits (Zhang et al., 2020). This meant reliable real time image transmission wasn't possible (Kim & Lee, 2021). Also, the PIR sensor occasionally gave false triggers when environmental conditions changed, for instance, with temperature shifts or other disturbances (Alam et al., 2020). Even with these limitations, the system clearly demonstrated its core functions: motion detection, alert generation, time based control, and communication (Gubbi et al., 2013). These results confirm the system's conceptual design and its feasibility, especially considering its modular architecture and event-driven operation (Banzi, 2011).

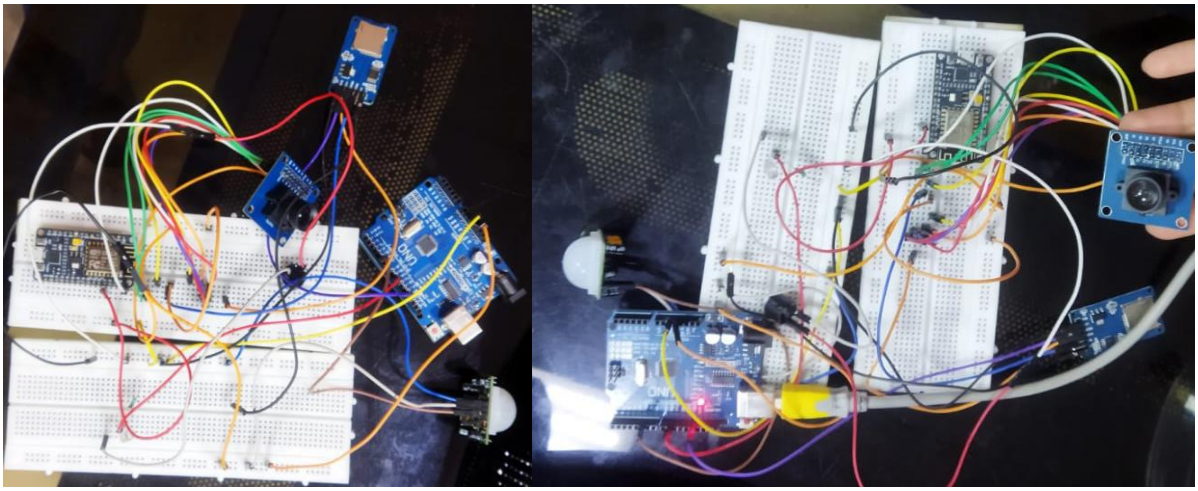

Figure 6&7: Set up of this project

## V. CONCLUSION

The Smart Intruder Detection System discussed in this research is considered one of the most efficient security systems available (Zhang et al., 2020). The idea behind the development of this innovative product has emerged from an interest in how real-time monitoring detects an intruder that tries to penetrate an area without being allowed at the specified time (Gubbi et al., 2013). The solution has been designed to incorporate a sequential alarm mechanism that makes use of the Arduino Uno along with the ESP8266 for creating a WiFi connection, and thus the automatic system operation is related to the association between automation and people's security needs (Borgia, 2014). In the framework of the effective and fully operational Smart Intruder Detection System, several technological components can be found, including a PIR sensor, an OV7670 camera, and others, in addition to the ideas about immediate response, escalation, and other (Kim & Lee, 2021).

## REFERENCES

[1]. Awajan, A. (Year). A Novel Deep Learning-Based Intrusion
[2]. Yaras, S., Kaya, M., & Polat, H. (Year). IoT-Based Intrusion Detection System Using Hybrid Deep Learning.
[3]. Ashiku, L., & Sivasubramanian, R. (Year). Network Intrusion Detection System Using Deep Learning.
[4]. Andalib, A., & Vakili, V. T. (Year). An Autonomous Intrusion Detection System Using Ensemble Learning.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15483

[5]. Alsubaei, F. S., Khan, M. A., & Rehman, A. (Year). Smart Deep Learning Model for Enhanced IoT Intrusion Detection
[6]. Sodhro, A. H., Kannam, S., & Jensen, M. (Year). Real-Time Efficiency of YOLOv5 and YOLOv8 in Human Intrusion Detection.
[7]. (IJISRT). (Year). Animal Intrusion Detection Using ESP32-CAM and YOLOv5.
[8]. Detection System for IoT Networks
[9]. Gayathri, M., et al. (Year). Object Surveillance Detection.
[10]. Bangali, J., & Shaligram, A. (Year). Design of a Smart Home Security System Using Object Recognition and PIR
[11]. D., et al. (Year). Intrusion Detection in IoT Using Image-Based Neural Network Classification.
[12]. Karthikeyan, R., & Prakash, S. (Year). IoT-Based Smart Surveillance System Using ESP32-CAM.
[13]. Patel, S., & Shah, N. (Year). IoT Enabled Intelligent Security System Using PIR and Camera Module.
[14]. Joseph Redmon, & Ali Farhadi. (Year). Real-Time Human Detection for Intelligent Surveillance Systems.
[15]. Kumar, A., & Singh, P. (Year). Smart Intrusion Detection System Using Computer Vision and IoT.
[16]. Rahman, M. A., & Islam, T. (Year). Vision-Based Home Security System Using Embedded Systems.

  