Journal of Electrical Engineering and Automation (ISSN: 2582-3051)
www.irojournals.com/iroeea/

# Automatic Smart Defense based Surveillance Security System using IoT

**Shankar Sharma K J.[1], Shoban Babu Y J.[2], Thanush Saran S.[3], Geerthana S.[4]**

[1-4]Department of ECE, K. Ramakrishnan College of Technology, Trichy, India

**Email:** [1]k.j.shankarsharma2004@gmail.com, [2]shobanbabu1007@gmail.com, [3]thanushsaran2004@gmail.com, [4]geerthanas.ece@krct.ac.in

## Abstract

The Automatic Smart Defense-Based Surveillance Security System is an advanced system proposed in this study to improve real-time security surveillance and eliminate danger. Traditional surveillance technology relies heavily on human interaction which, leads to inefficiencies, delays, and mistakes made by humans. To overcome these limitations, the proposed system uses radar technology, AI, and IoT to detect, monitor, and remove potential threats such as drone attacks and illegal activities. Automating the surveillance will reduce false alarms, minimize dependency on human involvement, and provide continuous monitoring with quick reactions. High-security areas, including military camps, border patrol zones, airports, and other important buildings are the most suitable for this system to enhance security.

**Keywords:** Automated surveillance, radar security, real-time threat detection, IoT-based security, AI-powered defense, drone interception, border security, critical infrastructure protection.

## 1. Introduction

As public and private safety issues have increased, researchers have made an effort to investigate different monitoring technologies that improve attack recognition and responses. Response latency is a feature of old technologies like closed-circuit television (CCTV) that mostly depends on human observation. The focus of current research has switched to machine


*DOI: https://doi.org/10.36548/jeea.2025.2.003*
*Received: 02.05.2025, received in revised form: 09.06.2025, accepted: 26.06.2025, published: 08.07.2025*

learning-based analytics, motion-detection cameras, and facial recognition. Although more accurate, these systems are still restricted by their dependence on centralized processing.

For example, the systems investigated in the research proposed by Sharma et al. [7] utilize cloud-based systems for image processing and facial recognition; however, these systems are unable to handle delays and lack the capacity for real-time decision-making. Similarly, Ahmed et al. [21] used a Raspberry Pi and ultrasonic sensors to create a motion-sensing surveillance system; still, it is not integrated into larger IoT networks or automated protective systems.

The Automatic Smart Defense-Based Radar Security System is designed to provide improved security and surveillance by quickly identifying, monitoring, and reducing possible threats. The system makes use of advanced radar technology to function effectively in a different application, including important buildings, battlefields, and borders. It offers effective tracking of attacks, illegal drones, and other dangers with quick and automated preventive measures. This proposed work aims to provide an efficient solution for current safety issues by reducing the limitations of traditional security systems.

## 2. Literature Review

For high-security locations, this research [1] proposed a complete Internet of Things (IoT)-based smart surveillance system utilizing sensors, cloud integration, and machine learning algorithms to provide real-time monitoring and decision-making processes. This work provided an effective solution for maintaining important facilities by focusing on high scalability, encrypted interactions, and automation in detecting attacks. The research [2] developed a smart surveillance and security system using a NodeMCU, PIR sensors, and cameras that could detect actions and send immediate alerts via email or smartphone notifications. The system appears to be more responsive than preventive because of its lack of autonomous defensive capabilities, although it is cost-efficient and effective in low-scale conditions.

In an IoT framework, Kodali et al. [3] Integrated home automation with surveillance, enabling users to remotely control appliances at home and to keep track of activities via a mobile application. When automation and security were implemented to improve user satisfaction, advanced threat analysis and response mechanisms were not included, and the

main focus was on household applications. A Raspberry Pi-based smart security system that used infrared sensors and cameras for recognizing intruders and live streaming video was established in this research [4]. Although the design supported remote monitoring, it was not possible to combine active defenses or react independently.

This methodology [5] designed a surveillance system based on infrared and ultrasonic sensors, highlighting the use of IoT to identify activity and illegal presence in sensitive places. It lacked intelligent processing features like object identification and behavioral analysis, but it was suitable for sending back simple intrusion alarms. A system designed for IoT defense that provides distant area tracking and oversight, particularly helpful in border and military monitoring, was introduced [6]. Currently, human response operations based on their work on environmental sensing and feedback loops provided the foundation for automated area monitoring. This research work [8] investigated CNN-based aerial monitoring with a specific focus on women's safety by reviewing aerial photos for illegal activity. The proposed application was restricted and mainly in computational format. This AI-integrated work showed the possibility of merging deep learning with IoT for preventive monitoring. Renuka et al. [9] implemented a protective robot-based facial recognition system for attack identification. The work operated within a limited robotic system, and this study mainly focused on automated responses to detected intruders, representing an improvement towards active security in smart surveillance systems. This proposed work [10] integrated cameras, sensors, and voice-activated assistants within the framework of their IoT-enabled home automation and surveillance system for the purpose of monitoring and managing home security. The system was efficient at communicating with users, but it did not provide sufficient space for automatic real-time responses.

This work [11] proposed an Internet of Things-based system for home automation and security using sensors and embedded controllers. Their research focused on user convenience and security, highlighting the advantages of remote monitoring and notifications in real time. However, the system was designed for home circumstances and did not include encryption of military standard or automated threat detection. A Raspberry Pi-based smart surveillance system for detecting movement and continuous video monitoring was presented by Mahesh et al. [12]. However, it lacked AI-based image processing or defense responses, which restricted its application in high-security zones; the cost and simplicity made it appropriate for small-scale operations.

Gavaskar et al. [13] employed the Internet of Things to create a real-time ATM monitoring and security system in order to prevent theft and unwanted access. The system integrated sensors with a communication module to provide real-time notifications. Its reactive technique limited preventative features like facial recognition or pattern-based attack prediction, considering its efficiency in breach detection. A smart video surveillance system was implemented in this method [14], using IoT to analyze and store videos in real time. Though the model's functioning remains ineffective due to the lack of autonomous decision-making or multi-sensor fusion, it highlights the importance of data accessibility and integrated observation. A protective surveillance robot with auto-combat systems and SONAR-based detection of intruders was introduced in this method [15]. With the ability to deal with attacks in real time, this approach indicated a shift from passive surveillance to active security. This study fails to deeply investigate the legal protections and strong environmental assessments. In this research discussion [16], the cybersecurity aspects of IoT-based smart homes highlighted possible flaws and AI-powered defenses. The present research increased the scope of monitoring by including cyber defense, which is important for securing communication lines and preventing device modification or illegal access.

A smart protection approach utilizing semantic evaluation for online security was explored in this research [17]. This model illustrated that AI and big data analytics could enhance the security framework, especially in multi-layered defensive structures, even if it was mainly directed at cyber-physical systems in smart cities. A smart border monitoring system that combines computer vision and wireless sensor networks was investigated [18]. This method significantly improved national security by allowing real-time tracking of attackers in remote border areas. The proposed analysis failed to consider autonomous weapons, scalability, or energy consumption.

This system [19], focusing on the development of IT frameworks for smart security, established an essential foundation for incorporating ICT into military systems. This study was mainly conceptual in nature and lacked useful details that support the idea of digitized military operations. The research [20] used delay-based detection techniques to address Network Time Protocol (NTP) security in defensive systems. The method improves the security and reliability of distributed protective networks, and time synchronization is essential in integrated surveillance systems.

## 3. Methodology

The proposed Automatic Smart Defense-Based Surveillance Security System combines a number of advanced technologies, including artificial intelligence (AI), the Internet of Things (IoT), machine learning (ML), and cloud computing for improved security monitoring and detection of threats. This approach uses a multi-layered architecture to provide automated, accurate, and real-time protection. Through the combination of ESP32-CAM, Arduino Uno, ultrasonic sensor (HC-SR04), and servo motor, the Automatic Smart Defense-Based Surveillance Security System is designed to offer real-time observation, intrusion detection, and auto-response [3]. The system uses AI-based monitoring and sensor-based detection to improve security and maintain continuous monitoring. The HC-SR04 ultrasonic sensor, which recognizes any kind of movement, activity, or restriction within its specified range, helps the system continuously scan the environment. When an item is detected, the Arduino Uno reads the sensor's data and performs a related action or alarm [4]. The ESP32-CAM allows for real-time surveillance through pictures or recording live video when it detects a threat. For the purposes of quick action or response, safety experts and organizations may examine this visual data remotely over WiFi.

Platforms for remote surveillance can easily include the security system. Security officers can keep an eye on the region in real time because of the ESP32-CAM's ability to stream live. To allow for quick action in the event of unusual behavior, the alarm can also be activated and sent to particular devices. The solution reduces false alarms and improves reaction accuracy by utilizing AI-based threat detection and automated tracking [5].

The accuracy of the ultrasonic sensor is confirmed by comparing the measurements with actual values, the servo motor's response time is evaluated to ensure smooth tracking, and power consumption is assessed to improve energy efficiency, making the system suitable for extended use without regular service [6]. Extensive testing is conducted to examine system performance under various environmental conditions, providing reliability for both day and night operations. The Automatic Smart Defense-Based Surveillance Security System provides an innovative approach to current security issues, ensuring additional security and constant monitoring with AI-driven technology and remote control. This smart surveillance system is highly adaptable and affordable, making it suitable for use in military defense, industrial security, and smart city monitoring.

## 4. System Architecture and Design

Multiple hardware and software layers are integrated into the architecture of an autonomous smart defense-based surveillance security system to provide extensive and intelligent security [figure 1]. The system's main component is a network with motion sensors, smart cameras, and environmental sensors that maintain track of the surroundings [8]. These systems record high-quality video feeds, recognize unusual motions, and detect changes in the surroundings, such as temperature or sound abnormalities based on the cameras used. The data collected by these sensors is transmitted to a central processing unit (CPU) or cloud-based server, where it is analyzed in real-time using advanced methods like artificial intelligence (AI) and machine learning (ML) to identify hazards or unusual behaviors.

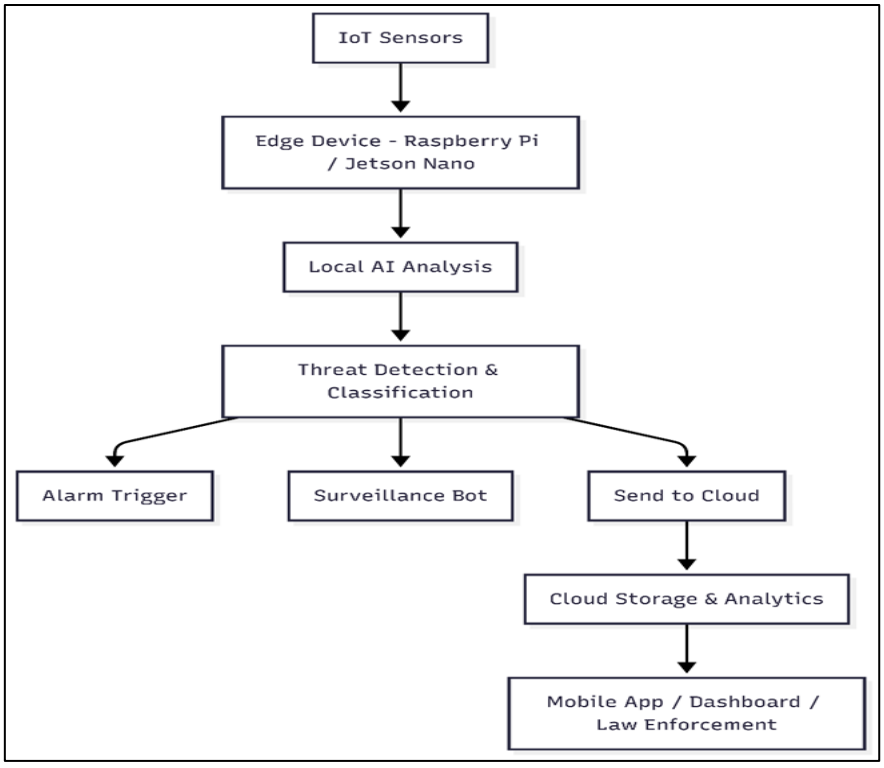


**Figure 1.** Architecture Diagram

A multi-tier technique is used in the system architecture to effectively handle data processing. First, the data is collected and locally pre-processed by the edge devices (such as cameras and sensors). This process helps the system make decisions more quickly and accurately in real-time by reducing latency and the quantity of raw data transmitted to the central system. The edge devices use basic algorithms for identifying anomalies to filter out unnecessary data, like background motions or environmental changes that aren't expected to be harmful or problematic. Deep learning models designed to detect particular safety concerns,

such as intrusion detection, weapon recognition, or abnormal human behavior, analyze the data more thoroughly after it has been delivered to the central processing unit.

The integration of automatic response systems is an essential part of the system's architecture. The system has the ability to initiate a sequence of operations that neutralize or reduce a potential danger. For example, if an intruder is detected, the system may immediately lock down access points, operate lights to avoid the attacker, and possibly send out real-time alerts to police or security officers [9]. Additionally, the system can interact with drones and other security devices to continuously track and monitor the suspect's movements. These measures can be modified to satisfy the specific needs of the surveillance area and are controlled by defined security regulations. The communication and data storage architecture is established to ensure that data is transmitted over the network in an effective and secure way. Confidential data is protected during transmission between edge devices and the central system when a secure communication technique, such as end-to-end encryption, is used [10]. For data redundancy, the system also includes backup servers or cloud infrastructure, ensuring that data remains accessible for additional analysis or inspection even if the main server location becomes unavailable. The system may expand into increasingly complicated and extensive environments because of its decentralized architecture, which ensures scalability and dependability.

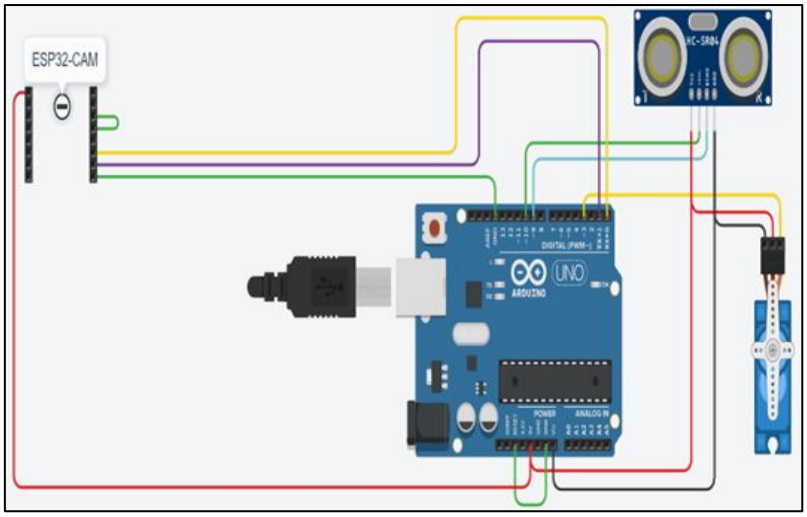


**Figure 2.** Circuit Diagram

Lastly, the reporting system and user interface (UI) are essential components of the entire design. Users or security staff may examine recent incident reports to observe real-time surveillance feeds and engage with the system via a user-friendly graphical interface. To assist operators in making well-informed decisions, the user interface includes situation dashboards,

maps, and warnings. Users can also manually override the automated responses when required. Figure 2 shows the circuit diagram of the proposed system.

## 5. Results and Performance Analysis

This system was deployed using Arduino IDE as the main programming platform. Arduino was utilized to code the microcontroller (ESP32-CAM) for managing the ultrasonic sensor, servomotor, and LED indicators.

- Important hardware components employed:
- HC-SR04 Ultrasonic Sensor for detecting obstacles.
- SG90 Servo Motor for scanning the environment in a 360-degree sweep.
- ESP32-CAM for live video transmission.
- LED for visual warning indication.

Simple interfacing with hardware components is provided by the Arduino IDE and libraries for ultrasonic sensing, servo motor control, and wireless communication using the ESP32 module. For simulation and visualization of obstacle detection, the project employs Processing IDE an adaptable software sketchbook and learning environment for coding within the context of the visual arts. The radar interface was implemented using Processing, which receives serial input from the Arduino (i.e., distance measurements from the ultrasonic sensor and servo positions), and graphs them in a half-circular radar format. This device proved handy for modeling real-time detection by showing red and green quadrants that change based on the presence or lack of obstacles, enabling real-time threat detection and response.

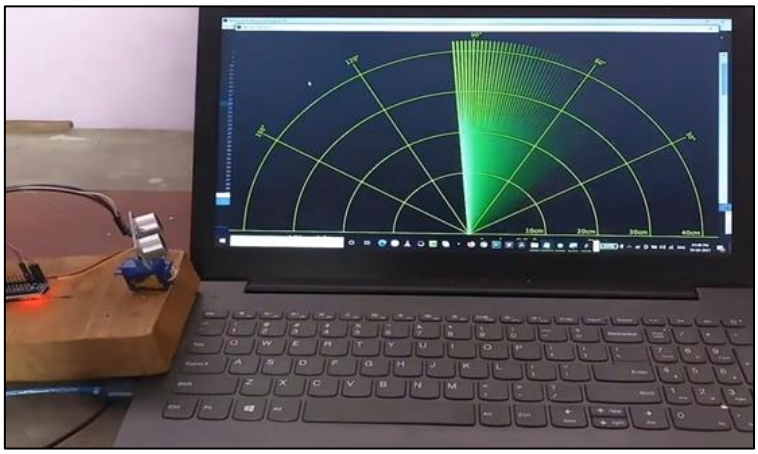

**Figure 3.** 360° Obstacle Detection using Ultrasonic Sensor with Servo Scanning

The system uses a 360-degree scan of the surrounding area with an ultrasonic sensor mounted on a servomotor, as illustrated in Fig. 3. Obstacles within the surveillance perimeter can be detected using this radar-based scanning technique. The scanned area and any obstacles found are visually indicated by the system's radar-like graphical user interface.

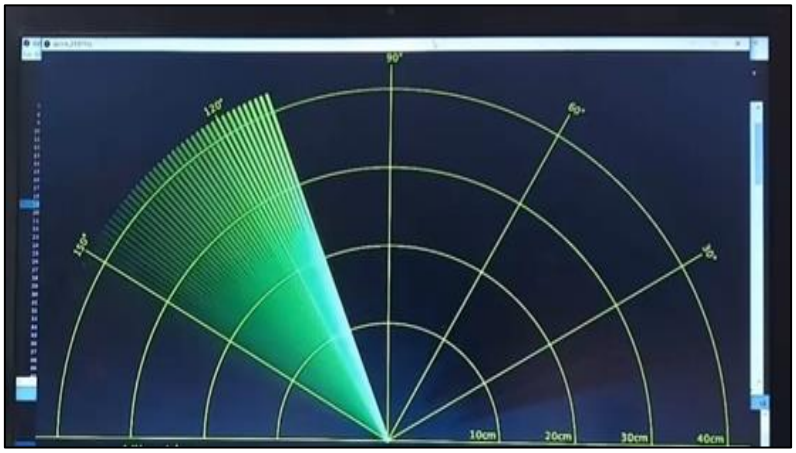


**Figure 4.** No Obstacle is Detected

In a clear environment, the radar interface shows only continuous green detection arcs, which means there are no obstacles in the way (Fig. 4). Nevertheless, the system visually confirms the threat or intrusion by highlighting the obstruction zone in red when an obstacle is detected (Fig. 5). This dynamic visualization guarantees timely responses and improves situational awareness.

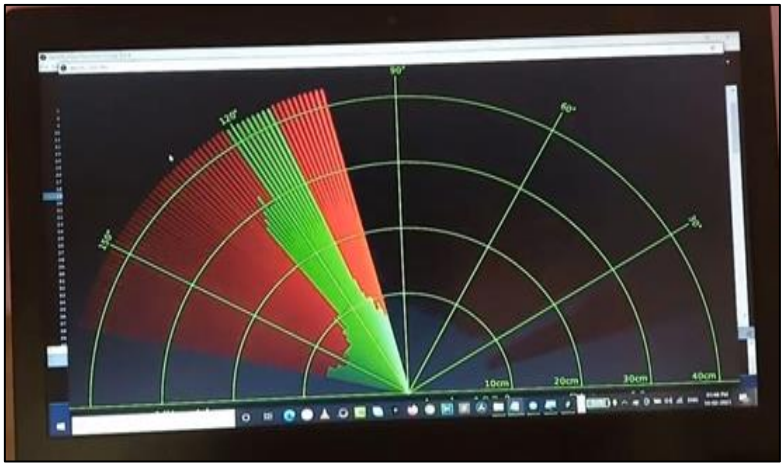


**Figure 5.** Obstacle is Detected and the Red Region Determines It

As shown in Fig. 6, the system also includes an ESP32-CAM module that creates a live video stream of the monitored area. This allows for real-time verification of the detected threat and remote surveillance. Incorporating live feed capabilities improves situational analysis and permits human oversight when required.

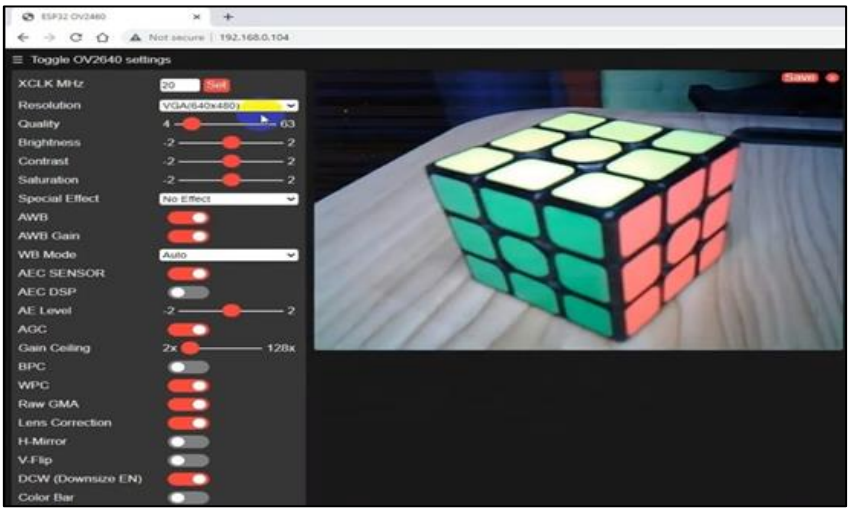


**Figure 6.** The ESP32-CAM is Making a Live Feed

Additionally, the system is designed to use an LED alert to initiate a warning mechanism. As seen in Fig. 7, the LED illuminates when the ultrasonic sensor detects an obstruction in the live feed and it shows the LED glows when the obstacle is detected in the live feed with the help of ultrasonic. This supports prompt on-ground action by providing an instant local indication of intrusion. A reliable, automated, and low-latency response system is ensured by the combination of radar detection, visual confirmation, and real-time alerts. This reduces the possibility of human error and boosts the overall effectiveness of surveillance in sensitive areas like military zones and critical infrastructure.

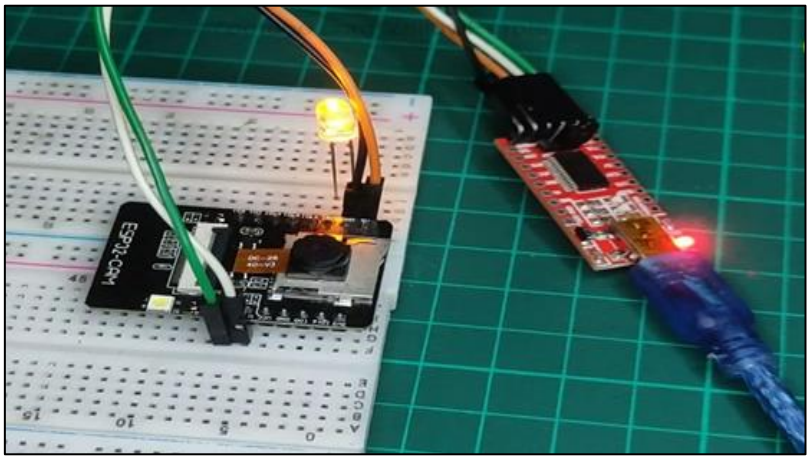

**Figure 7.** ESP32-CAM with LED Indicator for Obstacle Detection Sensor

## 6. Advantages

Using advanced radar technology, this system is a modern security solution that improves the tracking process. One of the main advantages is that cost-effectiveness leads to a

suitable method for various applications related to security. Additionally, it requires minimal maintenance and operating expenses, ensuring its durability without draining the budget. Radar technology is often used in advanced applications, such as NASA's mapping of Earth and planets, proving its dependability in challenging environments. Quick responses are another area where the system excels, allowing for immediate action against possible security threats. It is the appropriate solution for both private and public safety measures due to its affordability. The technology also ensures that all monitoring data is updated continually, offering real-time analysis for well-informed decision-making [20].

## 7. Conclusion and Future Work

The suggested system develops an efficient, autonomous surveillance system through the judicious integration of LED alerting systems, servo scan-based systems, ultrasonic sensors, and real-time video streams. The system enhances situational awareness and provides a timely response to potential threats through minimized human interaction and the utilization of radar visualization along with live-feed monitoring. An economical and scalable solution for areas requiring high security is enabled through the use of a Processing IDE in graphical simulation as well as the ESP32-CAM in Internet of Things-based video streaming. Due to its reliable obstacle detection, dynamic area coverage, and instant threat indication, the system can be implemented in sensitive regions such as military camps, border points, and important infrastructure centers. The system can be scaled for use in large-area security applications in the future by distributing multiple sensor nodes over broader areas. The incorporation of renewable energy sources, like solar panels, can enhance the portability and off-grid installability of the system, making it more versatile for a variety of real-world scenarios.

## References

[1] Afreen, Hina, Muhammad Kashif, Qaisar Shaheen, Yousef H. Alfaifi, and Muhammad Ayaz. "IoT-based smart surveillance system for high-security areas." Applied Sciences 13, no. 15 (2023): 8936.

[2] Lulla, Gurusha, Abhinav Kumar, Govind Pole, and Gopal Deshmukh. "IoT based smart security and surveillance system." In 2021 international conference on emerging smart computing and informatics (ESCI), IEEE, (2021): 385-390.

[3] Kodali, Ravi Kishore, Vishal Jain, Suvadeep Bose, and Lakshmi Boppana. "IoT based smart security and home automation system." In 2016 international conference on computing, communication and automation (ICCCA), IEEE, (2016): 1286-1289.

[4] Patil, Neha, Shrikant Ambatkar, and Sandeep Kakde. "IoT based smart surveillance security system using raspberry Pi." In 2017 international conference on communication and signal processing (ICCSP), IEEE, (2017): 0344-0348.

[5] Afzal, Muhammad, Muhammad Aoun, Shafiq ur Rehman, Muhammad Aftab Kaleem, Muhammad Jamil, and Muhammad Taqi. "IOT Enabled Smart Ultrasonic Surveillance System Using IR Sensor." Journal of Computing & Biomedical Informatics 5, no. 01 (2023): 391-402.

[6] Degadwala, Sheshang, Sabith Ahamed Musa, Dhairya Vyas, and Pooja Mitra. "IoT Defence: An Internet Based Remote Area Monitoring and Control System." In 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, (2021): 487-491.

[7] Sharma, Mukul, and Subhash Chand Gupta. "An internet of things based smart surveillance and monitoring system using Arduino." In 2018 international conference on advances in computing and communication engineering (ICACCE), IEEE, (2018): 428-433.

[8] Dandamudi, Aadesh Guru Bhakt, Gorrepati Vasumithra, Gangisetti Praveen, and C. V. Giriraja. "CNN based aerial image processing model for women security and smart surveillance." In 2020 third international conference on smart systems and inventive technology (ICSSIT), IEEE, (2020): 1009-1017.

[9] Renuka, B., B. Sivaranjani, A. Maha Lakshmi, and Dr N. Muthukumaran. "Automatic Enemy Detecting Defense Robot by using Face Detection Technique'." Asian Journal of Applied Science and Technology 2, no. 2 (2018): 495-501.

[10] Sanjay, A., Meenu Vijarania, and Vivek Jaglan. "Security surveillance and home automation system using IoT." EAI Endorsed Transactions on Smart Cities 5, no. 15 (2020): e1.

[11] Quadri, Syed Ali Imran, and P. Sathish. "IoT based home automation and surveillance system." In 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, (2017): 861-866.

[12] Mahesh, K., P. S. Ashok Kumar, H. N. Naveen Raj, P. P. Naik, and M. N. Apoorv. "IoT based smart surveillance security system using Raspberry Pi." IJARIIT 5, no. 3 (2019): 1356-1358.

[13] Gavaskar, K., U. S. Ragupathy, S. Elango, M. Ramyadevi, and S. Preethi. "A novel design and implementation of IoT based real-time ATM surveillance and security system." Advances in Computational Intelligence 2, no. 1 (2022): 1.

[14] Gulve, Sonali P., Suchitra A. Khoje, and Prajakta Pardeshi. "Implementation of IoT-based smart video surveillance system." In Computational Intelligence in Data Mining: Proceedings of the International Conference on CIDM, 10-11 December 2016, Springer Singapore, (2017): 771-780.

[15] Vadivel, M., S. P. Vimal, V. G. Sivakumar, V. Vijaya Baskar, and M. Selvi. "Internet based defence surveillance robot to prevent intruder activities and auto combat system using SONAR technology." In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), IEEE, (2023): 1055-1059.

[16] Appiah, Mayfred. "IoT-based smart home: benefits, risks, solutions, and the AI developments for cyber defense." (2022).

[17] Xu, Ning, Zheng Zhou, Jie Xu, Liang Dong, Wangsong Ke, Zhaoyu Zhu, Yuxuan Ye, Xiang Li, and Chao Huang. "Intelligent Defense Policy for Web Security Defense on Account of Semantic Analysis." In International Conference on Big Data Analytics for Cyber-Physical System in Smart City, Singapore: Springer Nature Singapore, (2022): 47-54.

[18] Bhadwal, Neha, Vishu Madaan, Prateek Agrawal, Awadesh Shukla, and Anuj Kakran. "Smart border surveillance system using wireless sensor network and computer vision." In 2019 international conference on Automation, Computational and Technology Management (ICACTM), IEEE, (2019): 183-190.

[19] Chung, Kyo-Il, So Yeon Lee, Sangjoon Park, Jonghyun Park, and Sang-Cheol Han. "Development of Information Technology for Smart Defense." Transactions of the Korean Society of Mechanical Engineers A 38, no. 3 (2014): 323-328.

[20] Dinar, A. E., S. Ghouali, and B. Merabet. "NTP Security by Delay-based Detection in Intelligent Defense Systems." Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 13, no. 1 (2021): 17-26

[21] Ahmed, Syed Umaid, Hamza Khalid, Muhammad Affan, Tauqeer Ali Khan, and Marium Ahmad. "Smart surveillance and tracking system." In 2020 IEEE 23rd International Multitopic Conference (INMIC), IEEE, (2020): 1-5