ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Implementation of an Integrated System for Surveillance, Monitoring and Security in a Compartment using the Internet of Things.

Raceforth Atori, Cletus Olisenekwu, Atori Raceforth

Science Laboratory Technology, Delta State University, Abraka, Delta State, Nigeria

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500049

Received: 30 April 2026; Accepted: 04 May 2026; Published: 28 May 2026

ABSTRACT

Security can be defined as the degree of resistance to, and resilience against, various forms of harm. It influences all facets of human existence, with infrastructure serving as a critical domain requiring robust security measures. Broadly speaking, security denotes a state of being free from threats and dangers, encompassing the protection of individuals and organizations against criminal activities such as terrorism, kidnapping, theft, piracy, and espionage. In the context of public transportation, particularly within train compartments, security is paramount to ensuring the safety and well-being of both passengers and cargo. In contemporary society, the lack of sufficient security measures on trains presents a significant concern for commuters. Issues such as theft, harassment, kidnapping, violence, and espionage have become increasingly prevalent among train users. The inadequacies of security personnel, coupled with the ineffective implementation of safety protocols, have exacerbated these challenges. Historically, the security framework aboard trains has been limited to basic measures such as lockable doors and windows, emergency alarm systems, and routine patrols conducted by train staff. The imperative for enhanced security and safety across both public and private sectors cannot be overstated. The development of various technological devices designed for the purposes of security has contributed substantially to improved safety conditions. Notably, the concept of safety extends beyond the mere physical protection of an organization to encompass an integrated approach to security.

In previous decades, security products were often designed with a singular focus; however, a significant evolution in security systems has been noted, particularly in residential and industrial sectors. Various technologies, including closed-circuit television (CCTV), Internet Protocol (IP) camera systems, and digital or network video recorders (DVR/NVR), have been deployed with the objective of enhancing security for properties and lives. Despite these advancements, concerns regarding the effectiveness and reliability of these systems persist. Although considerable innovation has been directed toward safeguarding lives and properties, the predominant strategy for ensuring security involves the implementation of surveillance and monitoring systems. Such systems, which consist of both hardware and software components, are utilized for the continuous observation of behaviours, activities, individuals, or locations in anticipation of criminal acts.

This surveillance process entails remote monitoring via electronic devices, such as CCTV cameras, as well as the interception of electronically transmitted information through mechanisms like passive infrared detectors, phone calls, and radio frequency. Effective monitoring necessitates round-the-clock observation performed by trained security personnel, who must be prepared to respond swiftly to potential intrusions from a safe distance. CCTV systems, often regarded as a panacea for security challenges, face inherent limitations when human oversight is absent. Factors such as human error, operator fatigue, and the potential for data tampering by criminals can undermine the efficacy of CCTV surveillance. The insufficiency of security personnel and inadequate safety protocols further exacerbate these vulnerabilities.

To address these challenges and to ensure comprehensive protection for lives and properties, there is a pressing need to develop integrated surveillance and monitoring security systems leveraging the Internet of Things (IoT). Establishing such an integrated video surveillance system for real-time monitoring, characterized by an

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

expansive coverage area that would empower control units to make well-informed decisions in mitigating insecurity effectively and.

The integration of advanced video camera sensors with computing capabilities has the potential to revolutionize the oversight of live events through automated analysis of captured footage. This technology operates autonomously, enabling the real-time monitoring of activities within a train compartment and proactively identifying potential failures via the Internet of Things (IoT). The IoT serves as a comprehensive network platform that facilitates the exchange of data, fostering communication and automated control among interconnected devices. Moreover, advancements in cost-effective technologies and protocols enable the practical implementation of IoT, thereby positively influencing human lifestyles, businesses, and industrial sectors. This technological paradigm facilitates the development of sophisticated smart systems and applications. Typically, the IoT system consists of a consortium of sensors, software, digital machines, and consumer-oriented products. Within the context of this study, the design includes gas leakage detection system that monitors air quality for multiple toxic and hazardous gases, such as methane, propane, butane, carbon monoxide, smoke, and liquefied petroleum gas (LPG), each of which poses significant health risks.

The proposed system comprises an ESP32-CAM sensor module, which integrates a video camera, a passive infrared (PIR) sensor module, and an MQ-2 gas sensor module, all embedded within the surveillance monitoring framework. The ESP32-CAM, serving as the video microcontroller, is designed to detect, capture, and record visual activity in the train compartment upon receiving a HIGH signal from the PIR sensor or a dangerous gas notification from the MQ-2 sensor. When implemented in a train compartment, this system serves a dual purpose: it acts as a gas detector and enhances security measures, thereby safeguarding lives, property, and facilities. Figure.1. demonstrated a global flamework and how they interacted with internet of all things network.

Fig 1. Demonstration of Internet of Things (Rakshitha et al., 2017)

Review of Related Work

This section elucidates various pertinent security systems proposed by researchers in the domain of smart surveillance. Numerous scholarly works have introduced innovative architectures and deployment strategies for smart surveillance systems leveraging Internet of Things (IoT) solutions. These systems typically comprise an array of sensors and camera modules designed to detect motion by capturing live streaming footage across various technological fields. The advancement and implementation of an integrated system for surveillance, monitoring, and security utilizing IoT have prompted a transformative shift compared to traditional surveillance methods and some contemporary intelligent designs.

Historically, conventional surveillance techniques included visual inspection, physical deterrence, human observation, physical barriers, and rudimentary alarm systems. It was not until the mid-20th century that the transition to electronic surveillance became a defining development in this field, marked notably by the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

introduction of closed-circuit television (CCTV). These early electronic systems utilized analogue cameras that transmitted live footage to monitors; however, their recording capabilities were limited, necessitating continuous physical monitoring by security personnel. Such requirements gave rise to challenges, including human errors in judgment, fatigue, the risk of data loss due to negligence, and inherent limitations in human visual perception [9]. In one notable study, an IoT-based automated home security system was developed utilizing a Raspberry Pi, strategically positioned at the primary entrance of a user's residence or office. This system is designed to send security alerts while simultaneously notifying users via email on their smartphones, irrespective of their geographical location [10]

Similarly, [11] and [12] contributions to the field involved developing an Ontology-based Context-aware IoT Framework for Smart Surveillance that processes live video from CCTV cameras to provide real-time alerts via SMS/email. In a study by [13], a home security system designed around the Internet of Things (IoT) is discussed. The author implemented this system using an Arduino Uno microcontroller, facilitating the interconnection of various components, such as a magnetic reed sensor, to monitor the status of a buzzer for alarm activation. The system's architecture incorporates the microcontroller's storage as the primary data repository, utilizing the internet for communication. A significant concern highlighted in this design is the vulnerability of internet connectivity to hacking attempts, which may compromise data integrity through unauthorized access and tampering on unencrypted platforms. Moreover, the author noted limitations related to the microcontroller's memory capacity, which is constrained to 32 megabytes. This relatively small memory size poses challenges for the system, especially when attempting to store data while simultaneously monitoring the status of the buzzer. The task of efficiently managing the limited memory resources while ensuring reliable functionality of the security device presents considerable complexities. This innovative IoT-based surveillance and security system combines sensors, cameras, and automation technologies, significantly enhancing security measures and efficiency. Real-time monitoring, it allows for swift responses to threats and sends automated alerts to authorised personnel, storing encrypted data on the Telegram platform. However, challenges include maintaining stable internet connectivity, securing sensitive data, and integrating various devices. Despite these issues, the benefits of the IoT system are evident.

As articulated in a study [14], hybrid edge-cloud smart surveillance systems have been developed using Raspberry Pi, NoIR (No infrared filter) cameras, and cloud computing to deliver IoT services while maintaining local inference at the edge device. The implementation of mobile-first solid-state devices (SSDs) and the MobileNetV3 model for object detection, deployed through Amazon Web Services (AWS), such as IoT Greengrass and AWS Lambda, allows the system to scale to thousands of surveillance nodes and relay notifications to users via the Amazon Simple Notification Service. Experimental validation has evidenced the system's efficacy in positively detecting people and animals in both diurnal and nocturnal conditions. Future iterations are poised to concentrate on zero-touch provisioning, scalability, and the optimisation of resource utilisation for devices with limited resources.

A review of related literature indicates a critical gap in the availability of a comprehensive security surveillance system that encompasses all requisite characteristics, particularly in relation to bandwidth requirements [15]. Additionally, the design of a decentralised platform for managing heterogeneous IoT networks underscores the pressing need for standard protocols to guide various IoT implementations within edge, fog, and cloud computing domains [16]. Existing gaps also persist concerning communication protocols at the application layer specific to video surveillance systems (VSS), necessitating future researchers to address these challenges to fulfil the protocol requirements effectively. An efficient VSS architecture must, therefore, be capable of accommodating devices ranging from resource-constrained IoT edge nodes to resource-rich cloud environments, while effectively managing the data generated across the edge, fog, and cloud layers.

Lastly, the proposition of a low-cost prototype for IoT-based smart monitoring highlights the potential for developing economically viable solutions utilising motion-triggered image-capturing technology in conjunction with Passive Infrared sensors (PIR). The work exemplifies the design and implementation of a prototype encompassing both hardware and software components, including camera motion alerts utilising advanced ESP32 microcontroller technology [17]. The integration of Internet of Things (IoT) technology into security systems has garnered significant attention in recent research. According to a study presented in [18], "An

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Ontology-based Context-aware IoT Framework for Smart Surveillance," continuous live video streaming and data captured by CCTV cameras can be processed in real-time to generate alerts for concerned authorities. These alerts can be disseminated via multiple channels, including email, SMS, on-screen notifications, and alarms.

Further advancing this concept, [19] reports on a study "Security Surveillance and Automation System Using Internet of Things," which outlines a dual-function system comprising home security and automation aspects. This proposed system includes a smart security camera module and an Android-controlled door lock. The camera, utilizing a Raspberry Pi coupled with a Pi camera, employs face recognition techniques through OpenCV to identify individuals lingering in front of the residence, subsequently sending the captured image to the homeowner via email. The Android door lock is operated through commands sent from a mobile device, allowing for remote locking and unlocking. Additionally, the home automation component consists of rain-sensing windows and automated lighting systems. The rain-sensing windows utilize a rain sensor to detect precipitation, autonomously closing when it rains and reopening only after the rain ceases. Infrared sensors are incorporated to identify occupancy within the home, triggering an LED to turn on in the presence of individuals, which subsequently switches off when the occupants leave. In a further exploration of security measures, [20] presents a "Wireless Intruder Detection System for Remote Locations." In this system, a motion sensor activates a digital camera only upon identifying an intrusion. The camera initiates recording and transmits video footage to a base station via Zigbee or Bluetooth transmission modules, where the received information is decoded for analysis. Moreover, [21] discusses the developments in "Intelligent Video Surveillance (IVS) Systems," which utilize analytic software to automatically detect relevant objects and security events within video footage. This innovation has emerged as a response to the constraints of traditional surveillance methodologies. Nevertheless, existing systems are still perceived to lack critical features, such as zone barriers, facial recognition capabilities, remote surveillance, and detection systems for power outages.

These studies collectively underscore the rapid evolution of IoT-based security systems, showcasing their potential to enhance both surveillance and automation functionalities in residential and community settings. However, a recurring limitation across these studies so far is the reliance of the researchers and authors on SMS, Bluetooth and email systems for manual monitoring and notification processes. The nature of SMS and email communication leads to potential delays in response times, thereby heightening security risks. Email, in particular, is susceptible to low-latency issues, as notifications may not be promptly checked or acted upon. Moreover, inbox clutter can result in the inadvertent oversight of critical alerts. Additionally, email communications are vulnerable to cybersecurity threats, including breaches and other forms of cyberattacks. Storage bottleneck breached. Running detection streaming often pushes memory to the limit, causing crashes due to storage space. Edge processing helps, but it's not perfect. Lack of swift real-time performance. This system requires more memory to accommodate extensive content storage. Utilizing a reduced memory associated with the MSP32-CAP for storage purposes adversely affects the system performance and efficiency. In this context, the Telegram platform is employed to facilitate the transfer and storage of large files or data. Telegram offers significantly greater storage capacity compared to MSP32-CAP memory at a lower or negligible cost relative to Firebase storage, end-end-encrypted servers. Access to stored data is extensively available through shared links or viewing invitations.

The innovative development of an integrated system for surveillance, monitoring, and security utilizing the Internet of Things (IoT) has marked a significant advancement in the field. This device amalgamates sensors, cameras, and automation technologies, thereby enhancing security measures, improving operational efficiency, and increasing the accuracy of threat detection. The real-time monitoring capabilities of the system facilitate prompt responses to security breaches, while automated alerts inform authorised personnel of potential threats. All data generated is securely stored on the Telegram platform, thereby providing a more robust solution compared to traditional systems. Nonetheless, the implementation of this IoT-based surveillance system has revealed several challenges, including the necessity for stable internet connectivity, safeguarding sensitive data against unauthorised access, and the successful integration of diverse sensors and devices. Despite these challenges, the advantages of the system are clearly delineated. The remote monitoring capabilities allow authorised personnel to oversee critical areas from virtually anywhere, while automated responses guarantee timely actions in the event of security incidents.

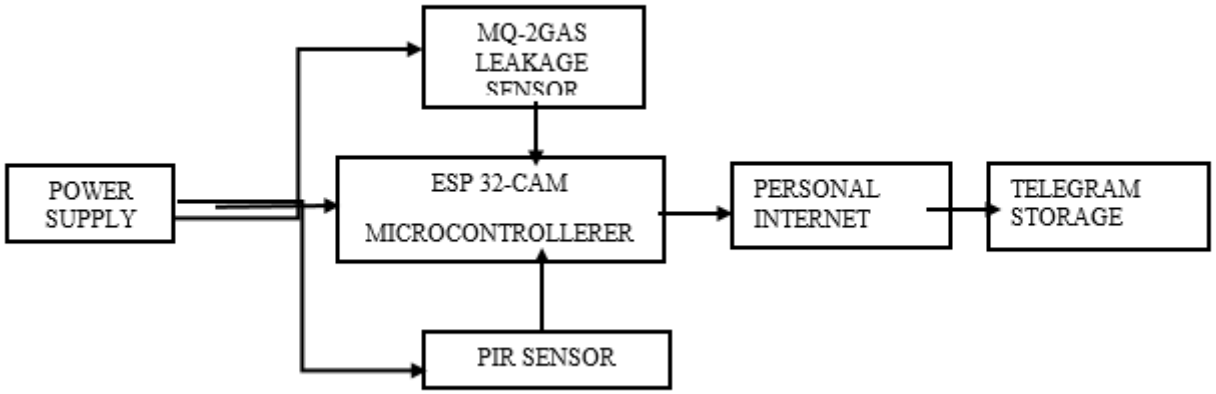
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

MATERIALS AND METHODS

Based on the requirements and architecture, the following hardware modules were selected for the design to ensure that all modules were compatible and could work together seamlessly. The ESP-32 CAM sensor, HC-SR501 PIR sensor, MQ-2 gas detector sensor, 3.7V lithium battery and TP4056 charging module. This project combines the above modules listed sensors to create a functional system. The ESP32-CAM module serves as the core processing unit, coordinating sensor data and video streaming. The HC-SR501 PIR sensor adds a layer of motion detection, allowing the system to identify and respond to movement. The MQ-2 gas sensor provides an additional layer of safety by detecting combustible and dangerous gas leakage. Powered by a rechargeable 3.7V lithium battery with a TP4056 charger, ensuring continuous operation. It captures real-time video, detects motion, and monitors air quality for gases like methane, propane, and carbon monoxide. The integration of captured videos, motion detection and gas leakage detection makes it a robust solution for monitoring and responding to potential threats.

Figure 2. The Block Diagram of the Monitoring Security System (Rakshitha et al., 2017)



Power Supply System

This system is designed to deliver a stable 3.3V power supply from a 3.7V lithium battery. The TP4056 module ensures safe charging of the lithium battery while preventing overcharging. The ESP-32 CAM was powered via USB from an external rechargeable lithium battery. During construction, a battery was used to ensure uninterrupted operation. The board functions optimally within a voltage range of 3.3V to 3.7V. Powering the system with a voltage lower than 3.3V may cause instability, while exceeding the maximum voltage of 3.7V risks overheating and potential damage. It is crucial to keep the voltage within the recommended range of 3.3V to 3.7V.

Power Supply Unit

The ESP32-CAM module requires a power supply of either 3.3V or 5V, which can be provided using a rechargeable lithium battery. Instead of a single 2000mAh battery, a dual configuration of 2000mAh batteries (2x2000mAh) was utilized. This approach significantly extends the runtime. Both batteries were selected from the same cell type and capacity and were connected in parallel to prevent higher voltage cells from overpowering lower voltage ones, thereby avoiding any risk of overheating.

The ESP32-CAM board is equipped with the ESP32 microcontroller, the OV2640 camera module, and a microSD card slot, facilitating various functionalities in embedded systems. This board operates with an input voltage of 5V DC, which is supplied through designated 5V and GND pins. Additionally, it is capable of functioning at a lower voltage of 3.3V, obtained directly from a 3.7V source, thereby enhancing its versatility in power supply options.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

The power consumption is 10 mA at 5V when idle or in deep sleep. When connected to Wi-Fi without the camera in use, the current draw increases to 350 mA (ACTIVE MODE). During active camera use with Wi-Fi streaming, the peak current reaches 700 mAh during Wi-Fi transmission.

Power supply for ESP32-CAM, PIR and MQ2 sensors.

The PIR sensor module and the MQ2 sensor modules require a 3.3V or 5V DC power supply, which is provided through a separate connection directly to the ESP32-CAM module

Input voltage: 5V DC, though it works 3.3V-5V. The sensor IC itself runs at 3.3V internally.

Current Consumption: 50 µA in standby and 100 µA when triggered.

Output: 3.3V HIGH or LOW signal on the OUT pin. (HIGH is motion detected, LOW is no motion).

Voltage Regulation: The voltage regulator regulates a stable 3.3V supply from the 3.7V battery received by the ESP32-CAM.

Battery Management: TP4056 Module manages the battery charging effectively and protects it from overcharging, overheating and ensures efficient energy use.

Battery capacity and Lifespan Calculation:

Power calculation for the ESP32-CAM sensor with a Lithium rechargeable battery of 2x2000mAh capacity.

To calculate the power requirement for the ESP32-CAM powered by a lithium rechargeable battery:

Active Mode: The ESP32-CAM consumes approximately 350mA when actively transmitting data or capturing images.

Calculation:

Runtime (hours) for ESP32-CAM + PIR+MQ-2 Load.

Batteries are rated in mAh at a specific Voltage. To get watts hours (Wh)

Wh = mAh x Voltage /1000.

2x2000 mAh at 3.7V.

Total mAh = 2000mAh + 2000mAh

Wh = 4000mAh x 3.7V = 14.8Wh.

With 85% boost converter efficiency,

Useable Wh = 14.8Wh x 0.85 = 12.58Wh

Continuous Operation 350mA avg at 5V = 1.75Watts

Runtime (hours) = 12.58Wh/1.75Watts = 7.2 hours approximately.

Pink Operation 700mA at 5V

700mA x 5V/1000 = 3.5Watts

Runtime (hours) = 12.58Wh/0.15W =84 hours (Approximately 3.5 Days)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

PIR- Triggered Operation:

ESP32-CAM sleeps at 50 µA and 100 µA only on motion, the MQ-2 heater is switched off 85% of the time, average load drops to approximately 25mA.

Runtime (hour) =12.85Wh/0.25W=51.4 hours.

However, using a 2000mAh battery capacity will not last as long as a 4000mAh battery capacity.

2000mAH battery with ESP32-CAM _PIR+MQ-2 setup

Total load of 350mA avg at 5V = 1.75Watts

Converting this battery into watts gives: 2000mAh x 3.7V/1000 = 7.4 Wh

At 85% efficient, approximately loo of 15% as heat is lost

Wh= 7.4Wh x 0.85 = 6.29 Wh

Runtime(hours) = 6.29Wh/1.75W = 3.6 hours approximately.

Peak of 700mA load when ESP32-CAM + MQ-2 both spikes.

Load = 5V x 0.7A = 3.5 Watts.

Runtime (hour) 6.29Wh/3.5W = 1.8 hours approximately.

Tab: 1. Table of comparison between 2x2000 and 2000 battery capacity and Runtime (hours).

Setup	Capacity	Continuous Runtime	Sleep Mode Runtime
1x2000mAh	7.4Wh	3.6 hours approximate	1.5 days approximately
2x2000mAh	14.8Wh	7.2 hours approximately	3.5 days approximately

2x2000mAh provides most of the working day on continuous recording. Utilizing 2x2000mAh battery capacity delivers more runtime than a single 2000mAh battery.

System Design

The system design comprises the requirements analysis, system architectural design and programming.

Requirements Analysis

The design began by identifying the key modules required for the surveillance and monitoring security system. After all the individual modules that will make up the system were confirmed for operational use, the system was set up to function as intended in the design. The primary tasks included video recording, detection of combustible and dangerous gas leaks, and sending real-time automated alerts.

System Architectural Design

The architectural framework of the device was carefully designed with distinct functional units, starting with the power management system. Key sensors for motion detection, video capture, and gas leak detection were integrated into a communication application, creating a comprehensive surveillance and security system within the Internet of Things (IoT) paradigm. This structure clarifies the interactions between the modules and highlights each module's specific role. The development process involved architectural design and software programming. Architectural design focused on ensuring effective functionality among the motion detector, video capture sensor, gas leak detector, and communication application. Software programming centered on

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

configuring the ESP32-CAM for motion detection, video recording, and Telegram bot communication, leading to a robust system that meets varied surveillance and security needs. Utilizing the Arduino Integrated Development Environment (IDE), the coding process facilitated the programming of the ESP32-CAM, PIR sensor, and Telegram bot functions. The functional block diagram (see Figure 2) illustrates component interactions and data flow, ensuring clarity. Additionally, software development included downloading necessary software, processing sensor data, controlling the camera, establishing storage solutions, and developing a web interface. Key features like encryption for secure data transmission and notification alerts enhance the system's security and functionality.

The ESP32-CAM microcontroller is mounted on a breadboard and powered by a 3.3-volt lithium battery for optimal functionality, as shown in Figure 3A. The PIR sensor and QM-2 Gas detector were thereafter connected to the ESP32-CAM in Figure 3B. The completed assembly was then placed in a plastic casing for testing in Figure 3C. Rigorous testing was conducted to ensure both functionality and security.

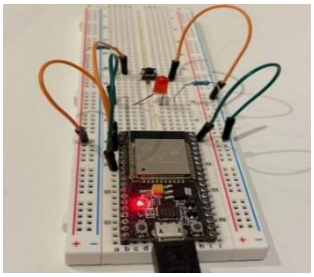
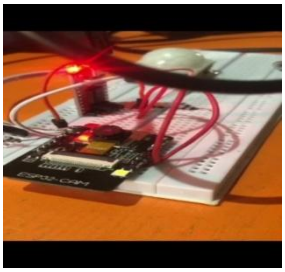




Fig. 3A. ESP 32-CAM on breadboard moved to plastic casing **Fig. 3B. PIR connected to ESP 32-CAM** **Fig. 3C. System setup**

Microcontroller Simulation/Programming

The software designed for the ESP32-CAM facilitates the execution of a diverse array of tasks, including but not limited to motion detection, video recording, gas leakage detection, and communication via Telegram Bot. The subsequent sections will delineate the key functionalities of the system, accompanied by relevant code snippets to illustrate these features. The initialization of the program commences with the establishment of a Wi-Fi connection, which is essential for the functioning of the various applications integrated within the system.

Software Implementation

In the plan of developing an integrated system for surveillance, monitoring and security, a meticulous journey was embarked on to ensure that every aspect of the software was robust and efficient. Here is the detailed account of the software implementation processes. The microcontroller Arduino IDE latest version was downloaded and installed from the official Arduino website.

System Setup

In the system setup, the serial communication, establishing Wi-Fi connection, the camera and configuring the sensors were initialized.

Code Structure

In order to ensure both clarity and functionality, the code has been systematically organized into distinct sections: initialization, the main loop, and auxiliary functions. This structural approach facilitates the individual addressing of each function while allowing for seamless integration within the overall framework.

Main Loop: The main loop continuously monitors the PIR sensor for motion and the gas sensor for gas levels. Upon detection of motion or a gas leak, the respective functions were triggered to handle these events.

Camera Initialization: This function configured and initialized the ESP32-CAM.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Capture and Send Video: This function captures a video and sends it to the Telegram-Bot.

Gas Linkage Detection: This function allows the gas sensor value to be read, and a notification is sent if the threshold is exceeded.

Telegram Bot Communication: This function is to send messages and videos to the Telegram bot.

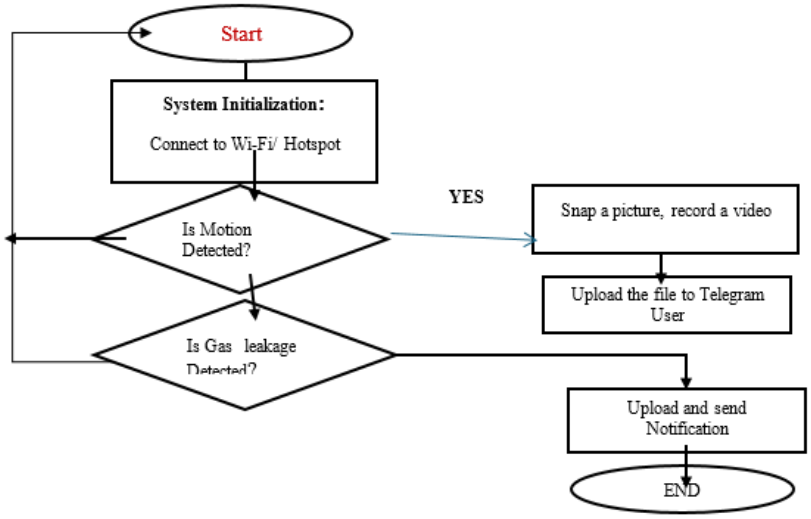


Figure 5. Schematic Diagram of the System Flow Chart

Mode of Operation

The system serves as a surveillance and security solution using the internet. It features a motion detection algorithm written in Python, implemented on an ESP32-CAM microcontroller, which enables live video streaming when movement is detected. The ESP 32-CAM is programmed to receive a HIGH signal from a passive infrared (PIR) sensor. When triggered, it captures motion, compresses it into a live video stream, and sends real-time alerts to the user via a Telegram bot. This information is securely processed and stored in Telegram, accessible only by the user or authorized personnel. Additionally, the system includes an MQ-2 gas sensor that monitors for hazardous gases such as methane, propane, and carbon monoxide. When these gases are detected, the MQ-2 sensor sends a HIGH signal to the ESP 32-CAM, which then alerts the user through the Telegram app.

Circuit Design

The circuit design was accomplished using Proteus 8 software, connecting all components and creating detailed schematic diagrams for each subsystem as part of the entire system. A proper voltage regulation system was distributed to ensure stability and reliability.

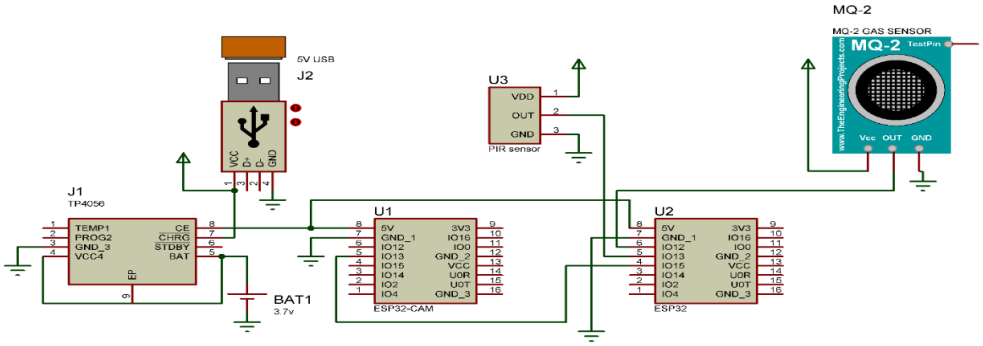


Figure 4: The Complete Circuit Diagram of the System

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

TESTING AND RESULT

The system, which combines software and hardware designed, underwent rigorous simulations and testing to ensure flawless operation. The circuit was divided into units, each tested meticulously. The lithium-ion battery produced an output of 3.7 Volts, with 3.3 Volts for optimal operation and 0.4 Volts for standby. The ESP32-CAM sensor captured images within 5 seconds at a range of 50-950cm, with diminishing quality beyond that. It provided reliable internet connectivity via Wi-Fi and hotspot, allowing for smooth live streaming and remote monitoring through Telegram. The HC-SR 501 PIR motion detector effectively identified movement within a 90–120-degree angle and a range between 4-30 feet, featuring adjustable sensitivity and a response time of about 5 seconds, while minimizing false triggers. The MQ-2 Gas Detector Sensor detected combustible gases but could not distinguish between them. Overall, the system's components performed as expected and met all requirements. Figure 6A displayed an image captured at a distance of 732cm in the laboratory and Figure 6B also displayed 153cm distance image captured during testing.

Fig. 6A. (732cm) distance captured image in a lab.

Fig.6B. (153cm) distance captured image.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

CONCLUSION

The implementation of an integrated surveillance monitoring and security system utilizing the Internet of Things (IoT) in train compartments presents numerous security advantages. This system enhances safety through real-time monitoring, enabling rapid responses to security breaches. Smart sensors and cameras work in unison to deliver comprehensive security coverage, detecting potential threats and promptly alerting authorities via the Telegram platform. The automated monitoring capabilities of the system minimize manual efforts, allowing resources to be allocated to other important tasks. Moreover, IoT-enabled systems can analyze data to identify potential security threats, facilitating proactive measures. Remote access to the system further enhances flexibility and response times, enabling authorized personnel to monitor and address security incidents from virtually anywhere. Customizable alerts and notifications ensure that relevant parties are promptly informed, significantly reducing the risk of undetected security breaches. Ultimately, by leveraging IoT technology, organizations can establish a robust, efficient, and effective surveillance monitoring and security system for train compartments, fostering a safer and more secure environment. As technology continues to advance, I strongly recommend that future developments in this system include the integration of artificial intelligence (AI) to improve threat detection and predictive analytics, the incorporation of additional sensors for enhanced monitoring, and the creation of a more user-friendly interface for streamlined system management. Furthermore, expanding the IoT-based integration to encompass other devices will contribute to a more comprehensive security ecosystem.

REFERENCES

1. **Myriam, D. C.,** Mareile, K., and Kristian, S. K. (2015), Resilience and (in) security: Practices, Subjects, and Temporalities: Research Gate. (Security Dialogue) 46: 120-125
2. **Adeleke, A.** (2013), Insecurity: A threat to human Existence and Economic Development in Nigeria, Research Gate. 6: 8-13.
3. **Sun, Y.,** Xiaogang, W, and Xiaoou T (2013). Hybrid Deep Learning for Face Verification: IEEE Transactions on Pattern Analysis and Machine Intelligence 38, (10)
4. **Lyon, D.** (2001). Surveillance Society: Monitoring in Everyday Life in Philadelphia: Open University Press. ISBN 978-0-335-20546-2
5. **Torin, M.,** David, M. and Wood (2018), Surveillance Studies: New York: Oxford University Press. ISBN 9780190297824
6. **Okpeki, U. K** (2018), Design and Construction of A Smart Security System: Journal of Sustainable Technology, 9, (1): 25-36.
7. **Ramya, G.,** Ramkumar, G., Anitha, G., Thandaiah. R., Nirmala.P. (2022): Strong and stable data communication using artificial intelligence method in mobile Ad-Hoc networks: International Conference on innovative computing, intelligent communication and smart electrical system (ICSES), Pp 1-25.
8. **Rezwanul, M.,** and Mohammed, A. M. (2020), Current Research Trends on cognitive Radio-Based Internet of things toward cognitive internet of things Network: (2): 5-17.
9. **Okpeki, U. K**, and Oyubu, A.O. (2021): Design and implementation of an integrated pipeline security system with optimised scheduling: Journal of Informatics and Communication Technology, 10 (1): 25-36.
10. **Ruby, D.,** Deepthi, U. S., Mohammed, M. A., Riya, M. A. and Abhishek, Y. (2018), IoT-Based Home Security System Using Raspberry Pi: International Journal of Innovative Research in Computer and Communication Engineering, 6,(4): 3835-3842.
11. **Nisha, P.A.,** Mallik, S and Chaudhury, (2018). An Ontology-based Context-aware IoT Framework for Smart Surveillance: Symposium on Computer Animation 3rd International Conference on Smart City Application. (69)**:** 1-7.
12. **Milind, R.,** Rampure. K. P. Rathod. K. M., Kamble. P, V. (2022), IoT-Based Smart Surveillance and Automation: International Research Journal of Engineering and Technology 9,(4): 3253-3256.
13. **Anitha, A.** (2017). Home security system using internet of things: IOP Conference Series: Materials Science and Engineering, 263: 1-11.
14. **McBride, G.** and Sumbwanyambe, M. (2021), Design and Construction of a Hybrid Edge Cloud Smart Surveillance System with Object Detection: International Conference on Computing, Communication, and Intelligent Systems, Pp 642-647.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

15. **Skrbic, B. D.,** Radovanovic, S., Tomovic, L., Lazovic, Z.Z, and Radusinovic. I. (2018), A decentralised platform for heterogeneous IoT network: Scientific-Professional Information Technology Conference.
16. **Chernyshev, M., Z.,** Baig, Bello, O. and Zeadally, S. (2018), Internet of Things Research, Simulators, and Test beds: Internet of Things. 5(3): 1637–1647.
17. **Prathima, S.K.,** Sivachandar, N.G., Praveena, C., Nithiya,D., Kamalesh, C.L. (2023), Low-cost Prototype for IoT-based Smart Monitoring through Telegram: 5th International Conference on smart system and inventive Technology.
18. **Nisha, P.A.,** Mallik, S and Chaudhury, (2018). An Ontology-based Context-aware IoT Framework for Smart Surveillance: Symposium on Computer Animation 3rd International Conference on Smart City Application. (69)**:** 1-7.
19. **Sanjay, A. M.** V. and Jaglan, V. (2020), Security surveillance and home automation system using IOT: EAI Endorsed Transactions on Smart Cities, Pp 165-963.
20. **Mrunal,** Khadkar, Asutkar, Gajendra, Hariprakash. R (2021): Wireless intruder detection system for remote location: Turkish Journal of Computer and Mathematics Education. Gurgaon. vol. 12, iss12. Pp 1390-1401.
21. **Kumar, A., Hashmi,** H., Khan, S. A. and Naqvi, S. K. (2021), A Smart Framework for Live Video Streaming based Alerting System: 10th International Conference on System Modelling & Advancement in Research Trends, Pp 193-197.