

Internet of Things (IoT) Based Real-Time Smart Security Surveillance System for Motion Detection

TIJJANI AHMADU SANUSI¹, PROF. PETER B. ZIRRA²

^{1,2}*Department of Computer Science, Faculty of Science, Federal University of Kashere, Gombe State, Nigeria*

Abstract- *The increase in IoT technology has paved the way to tremendous improvement in security systems especially in the application of motion detection smart surveillance. This paper describes the proposed an efficient IoT-based real time smart security surveillance system for protection of residences and commercial places. Advanced component sensors such as PIR sensor, GSM module and microcontroller have been used to realize a more realistic motion detection to trigger phone call and SMS alert. Extensive performance testing indicates high detection accuracy measured with confusion matrix and achieve high result i.e. 98% accuracy success rate with lower false alarms in day light and 95% under night conditions, which demonstrates efficient motion detection system. Moreover, system's proficiency is achieved by implementing various functionalities to ensure a robust system performing correctly in changing situations. Also this application has contributed positively for security management system against breaking with lower error and can work in any climate condition. By utilizing wireless communications and internet; these works lead to a wireless security and reduce dependency of human on traditional security system which have some disadvantages in regard to time and accuracy. This study is mainly focuses to provide higher level of security by reducing the danger of crime through utilization of IoT's smart security technology. Result of this work shows the effectiveness of IoT-based intelligent security system on improving real time response to any break-ins, hence it is a valid method for reducing crime threats in society. Further work to add high-level intelligence in order to improve distinction between objects is planned, besides providing scalability features for large deployment to fit in Smart city environment.*

Keywords: *Internet of Things (IoT), Passive Infrared (PIR) Sensor, Smart Security, Real-Time Surveillance, GSM Module, ESP32-CAM.*

I. INTRODUCTION

Security and safety are of great concern across many domains, thus enabling the rapid research and development of new surveillance technologies in

security monitoring systems. Among them, the Internet of Things (IoT) has emerged as the extremely impactful domain, influencing even the daily lives and the behavior of people along with the remote perception of physical entities (Sharma, 2023). As a statistical matter, the network of devices is evolving at an unmatched pace, there existed 14.3 billions active IoT connections on 2022 and estimated 16% increased number to 16.7 billions active nodes on 2023, where the active devices are further predicted to reach 29.7 billions by 2027 (Hercog, 2023). As an integrated environment of IoT, an 'Thing' is basically an embedded device equipped with electronic parts, actuator, sensor, and micro-controller to form a miniature node to gather and process information and transmit wirelessly to anywhere in the world to perform efficient and wide range of surveillance (Gavaskar, 2022). Additionally, the desire for learning the concepts of IoT led scholars and industrial to implement the idea in special applications and domains, so as to achieve an active control of systems. At the same time, the detection of motion has evolved and become a vital scientific and engineering sector (Gabriel and Kuria, 2020). In the past few decades, the incorporation of microcontrollers along with passive infrared (PIR) and ultrasonic modules has enabled excellent motion and proximity measurement (Franklin, 2021). Currently, monitoring human movement at a distance requires minimum effort as well as higher safety level and safe is defined as being free from danger, crime and loss (Iyapo et al., 2018). The addition of pir sensors along with IoTs enables real time monitoring and quick distribution of warnings (Sinha et al., 2022). Modern set-ups incorporate PIR sensor in combination with esp32 microcontrollers for transmitting of alert messages to social communication devices such as telegram thereby proving it as possible to implement for portableIoT monitoring (Gauhar et al., 2023).

Moreover, algorithms such as double-frame difference together with background modeling have been used in automated emailing upon detection within 1.64 seconds under conditions with changing lighting parameters (Ahmed et al., 2023).

1.1 STATEMENT OF THE PROBLEM

Crime such as theft, robbery and vandalism worldwide is still rising; there is growing concern over public spaces from people within both public and private sectors (Muhammad et al., 2019; Victor et al., 2023). The criminals are applying much more technical methods hence the need for adaptable and proactive counter measurements. Smart intrusion detectors had been conceptualized utilizing methods that involve web-enabled notifications, e-mails and local WiFi systems (Ayush and Joshi, 2012; Nwalozie et al., 2015; Arun and Saravana, 2021; Yuda et al., 2021; Usiade and Adeoye, 2022; Arinde, 2023) however there is a lot that seems to have been left out. Most critical of all, most of the system designed required 24/7 connection to the web (WiFi, e mail and instant messaging systems), system could be down if it can't reach internet in areas or if it can't reach grid if power is down. Secondly most security systems don't have backup with local alarms, direct cellular call and SMS as they only make alerts on phone messaging/applications. However this system takes images and make Cellular calls and SMStexts from another GSM module, therefore making it more cost effective, dependable, power-backup, avoiding phantom calls by using multi technology.

1.2 AIM AND OBJECTIVES

The main goal is to design, build and execute an IoT-based real time smart security surveillance technique which can detect motion. For fulfilling this goal, the following specific objectives have been set.

To design a multisensory real time smart security surveillance architecture with PIR Motion Sensor, Acoustic Sensor and Magnetic Switch Sensors.

To build and implement a physical model with Arduino Uno board and ESP32-CAM module.

To compare the implemented system performance empirically which reflects the precision of motion

detection, latency and reliability under both day and night condition.

1.3 SIGNIFICANCE AND SCOPE OF THE STUDY

This study's importance is how it can establish economical, smart surveillance. Employing inexpensive, ubiquitously available sensors such as; PIR motion sensor, sound sensor and a magnetic reed switch tied to a central microcontroller, the use of two redundant alert paths (GSM cellular and Telegram IP channels) enables cost affordable access to a system that would otherwise only be available to individuals with the capital available for a high-quality security network. This redundant system does allow a user to be notified of intrusion through a direct mobile phone call and through text message even when there is no local wi-fi, thus limiting response time. This study's scope in particular, addresses sensor interfacing and design, software development within the Arduino IDE, threshold settings development/calibration, physical case design and fabrication, and quantitative analysis via means of a confusion matrix.

II. LITERATURE REVIEW

Surveillance systems are interconnected frameworks of devices used for continuous observation, tracking, and recording of the state of the environment (Tsakanikas et al., 2018; Kadir, 2023). Historically, surveillance was passive; security guards were supposed to monitor hundreds of live CCTV screens simultaneously and report unusual occurrences without fatigue or making mistakes (Velasin et al., 2017). The advent of digital interconnectivity, Artificial Intelligence (AI), and edge sensors shifted surveillance toward an intelligent paradigm capable of real-time threat identification, object tracking, and automated alarms (Bhatt et al., 2017; Iyer et al., 2020). These intelligent video surveillance systems rely on deep learning algorithms while IoT surveillance networks coordinate the collected data by centralizing many distributed sensors (vibration, magnetic, acoustic, optical, thermal, etc.) and transmitting the correlated alerts to a central repository (Liu et al., 2019; Zhang et al., 2020). Despite the extensive security benefits these systems provide, such as quick detection of threats, minimized response times to events, efficiency through automation, and increased

cost-effectiveness in the long run smart security systems present a number of critical challenges including security against hacking, integration limitations of systems from different manufacturers, and the burden of managing large data volumes while complying with data privacy and other regulations (George, 2024; Pantuvo and Oluwarore, 2024; Zahid et al., 2023; Okolo et al., 2024).

2.1 REVIEW OF RELATED WORKS

A comprehensive review of related literature indicates a diversity of methods have been proposed to overcome difficulties in intruder detection. In commercially based security systems, an IoT based ATM intrusion monitoring systems was built using vibration sensors to detect any physical assault on an ATM by Gavaskar et al., (2021). It also involves blocking any further operations, activating door locks and throwing a remote controlled chloro spray. However, it depends on manual operation to function and risk of sensor error can still occur.

In household automation area, it was suggested by El-Shenawy, (2023) that we build a system to control ambient parameters using NodeMCU and Wi-Fi but it fails as it demands an internet connection at all time of high bandwidth. As far as the visualization and tracking aspect is concerned Gauhar et al., (2023) used ESP32-CAM and P IR sensor to upload captured JPG images to Telegram directly which is directly related with the idea of the camera part as mentioned above. Al-Hashemi et al., (2024) propose a 3 frame differencing algorithm on video to decrease any redundancies, while Kolaskar et al., (2021) used a dual stream C3D network which focuses on fusion of motion optical flow and space images but achieves a higher AUC score (90.37) at the cost of intensive processing which does not allow for execution on microcontrollers. Al-Slemani et al., (2023) used motion detection using AForge.NET with image classification using Tiny YOLOv2 on the developed PC application and stated detection rates were as high as 95 percent but did not offer any advantages to desktop or mobility issues.

Usage of OpenCV as a feature extraction method achieved decreased consumption of CPU at 29.2% and RAM by 46.7%. Low cost boards such as a Raspberry

pi were seen being used by Bhakti et al. (2019) to perform activated recorded based on the motion detected but at present the main issues remain on the amount of high components and expensive systems for commercial deployment.

2.2 SUMMARY OF RELATED WORK AND RESEARCH GAP

Despite previous extensively researched advanced image processing systems and expensive sensor networks, there is little research focusing on a low-cost, low power-consumed security device that will work when the network connection fails. Mostly existing designs depend heavily on fast network connections (WiFi/cloud) for reporting, a scheme which fails readily when lines can be easily cut. During the normal power grid failure situations, existing solutions will cease to work.

It is also found that the existing studies rarely provide in-depth discussion on an effective integration strategy with local acoustic sensors (sound intensity sensors) and magnetic door contacts beyond PIR motion detection with minimum false alerts under one single cellular-calling GSM system.

This paper presents a physical prototype research that integrates sound intensity, magnetic state variables, PIR motion variables and uses an independent GSM device (SIM800L) to set up backup cellular links, independent of a usual Telegram display transmission.

III. METHODOLOGY AND SYSTEM DESIGN

This research uses an empirical experimental method of design, prototype and systematic test of proposed integrated IoT smart surveillance system. The primary data collected by physical sensor and logged quantitative test. The proposed system has a concentrated hardware which all the data signals from different heterogeneous sensors connected to a single central microcontroller (Arduino Uno- Atmega 328), processing all the alerting functions.

3.1 PROPOSED HARDWARE ARCHITECTURE AND INTERFACING

The hardware interface consists of five modules attached to the central Arduino processing board. They consist of:

1. Arduino Uno (ATmega328) Microcontroller: this acts as the brain of the security system, processing information from each of the sensors. It uses logic with a 5v supply and contains I/O pin outputs (analog and digital) in order to set sensor trip points activate the buzzer or issues serial command codes to the GSM receiver. It is powered solely by an in-built rechargeable battery at 4200mAH (10.8v). This allows security to continue with no problems even when power supplies are not available. In the context of an IoT-based real time smart security surveillance technology, the Arduino microcontroller board is an

open-source electronics prototyping platform based on a flexible, easy-to-use hardware and software, intended for artists, designers, hobbyists and any one interested in developing interactive objects-its physical computing platform (simply stated as) (Figure 3.5 displays the Arduino microcontroller board) is a small microcontroller board with a USB plug allowing it to connect to ones PC and a series of electrical connection points. These can be interconnected to external circuits namely; motor relays, light sensors, diodes, speakers and microphones etc. These can be powered up either through the connection sockets and the serial connection from the pc or through a 9v battery. they also can be remotely controlled from the computer or independently programmed and disconnected.

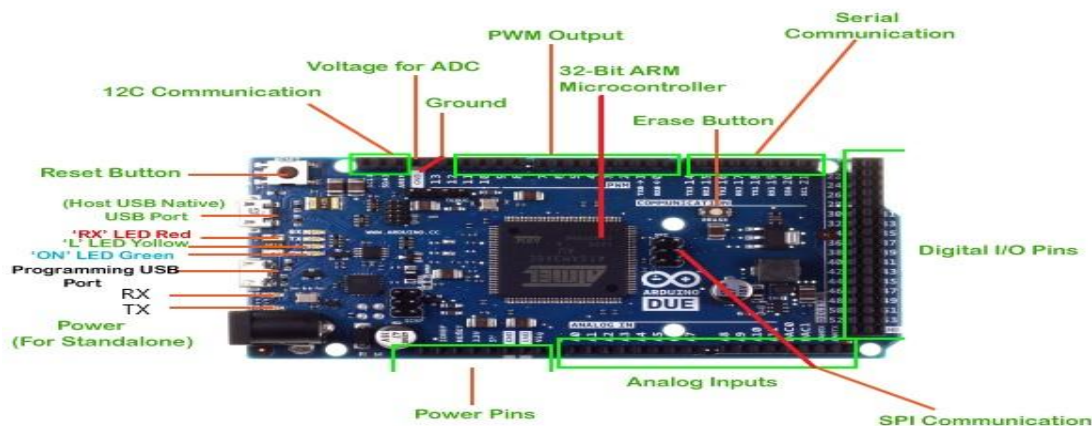


Figure 3.5 Arduino Microcontroller board

2. PIR Motion Sensor: A sensor used for detecting thermal motion across a large area. It detects any change in infrared radiation output from warm-blooded animals. It uses a field of view up to 90 degrees. Vcc is connected to arduino 5v, Gnd is connected to arduino Gnd, and the high signal digital output pin is connected to Arduino Digital Pin 7.

3. ESP32-CAM Module: A low cost, small board that contains Dual-core 32-bit LX6 CPUS, a OV2640 camera, Fully compliant WiFi and Bluetooth standard. Act as the individual network controller. When a trigger pulse is received from arduino via GPIO13 (as

PIR status pin). ESP32-CAM captures a JPEG picture as FRAMESIZE_SXGA resolution (1280x1024pixel) and sends to registered telegram group through secure SSL TCP connection.

4. Sound Sensor (peak detection and amplifier): Integrates with one on-board Capacitive Microphone, one LM393 comparator and one peak detection circuit, in order to trigger the unauthorized noise signal. Arduino digital input pin number 8 is configured for the sensor's high signal input (threshold determined by the decibel) to trigger the alert.

5. GSM Module (SIM 800L): A Quad-band GSM/GPRS module used to send messages/alerts via SMS utilizing UART serial communications over the 4 necessary wires: Tx, Rx, VCC, GND. SIM800L's Tx port connects to Arduino's Rx(Pin 0) and SIM800L's Rxport connects to Arduino's Tx(Pin 1). It requires a 5V regulated supply capable of supply peak GPRS transmission current up to 2A.

3.2 PRINCIPLE OF OPERATION AND SOFTWARE FIRMWARE FLOW

The system's workflow has dual paths of redundancy in terms of alerts and has false-alarm filtering. The complete workflow of the system shown as an operational flowchart in Figure 3.12 of research:

1. Bootup State: ATmega328P initially disables brown-out control in register controls and enables the serial port. It initializes EEPROM (utilizing 2 bytes for persistent storage of system state).
2. Sensor Initializing State: PIR sensor enters its initializing 30 sec time(progress gets printed to serial and boots alert in Telegram) , ESP32-CAM connect to pre-set SSID(IOT_Wifi).
3. Monitoring state: Microcontroller continuously checks for the status change for PIR sensor (Pin 7), Sound sensor (Pin 8) and switches' state.
4. Trigger State and Alarm sequence: Trigger condition occurs, If motion, sound or break contact occurs system runs a low power 10.8V battery driven piezo buzzer alarm, turns ON camera flash(GPIO 4) and run a GSM calling function.
5. Sending GSM alerts: Arduino commands SIM800L using AT series commands. After enabling text mode(AT+CMGF=1), send an SMS to registered number using command AT+CMGS, also makes a direct voice call to the concerned person with registered numbers in calling part simultaneously.
6. Capture image and sending to Telegram: Trigger ESP32-CAM to take image(with/without flash depending on current light condition) connect securely using a TCP

connection to api.telegram.org:443 and uploads the captured jpeg picture in multipart http post boundary POST /bot/sendPhoto, once upload completes with a confirmation the concerned user is notified on his/her Telegram app.

3.3 STATISTICAL ACCURACY AND CONFUSION MATRIX FORMULATION

The implemented confusion matrix is a binary one to quantitatively estimate the system performance, and to filter fake alarms. The states are defined into four: True Positive (TP): the detection of motion/pressure is correctly identified; True Negative (TN): stable state is correctly identified; False Positive (FP): false alarm is produced due to ambient disturbance; False Negative (FN): motion/pressure is not correctly detected. Mathematical detection accuracy of the system is expressed by:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

Furthermore the percentage error (error rate) is calculated as a proportion of incorrect decisions from the total number of tests and measured as follows:

$$\text{Percentage Error} = \frac{FP + FN}{\text{Total Cases}} \times 100\%$$

The Average response latency (in ms) calculated measures time elapsed between the real precise date time where event is logged until the time alert received by the user interface taking into account sensor detection in the edges, local processor (microcontroller) logic and through wireless GSM/GPRS/Wi-Fi network propagation

A diagram illustrated flow chart below shows the flow of the information systems modeling process components of existing system. Following figure 3. 11 shows the flowchart of operations:



Figure 3. 11 Flow chart of the existing System (source Gauhar et al., 2023)

Figure 3. 11 shows the flowchart diagram of the existing system showing the flow of operations and activity updates. Initially the system waits for motion being detected via the Passive Infrared (PIR) sensor. If there is no motion then the system waits again for a short while to then check again. If there is motion, it should immediately begin taking a photo from the ESP32-CAM and then turn on the light if necessary. A photograph is then either taken with a flash on or off depending on the conditions at the time. This

photograph is then sent to a pre-programmed Telegram account, that anyone can use to monitor the system at any time, to whoever the picture needs to be displayed.

A data flow diagram is a picture which explains how data flow is distributed within an information system. In Figure 3. 12, you are shown the data flow operations of the system.

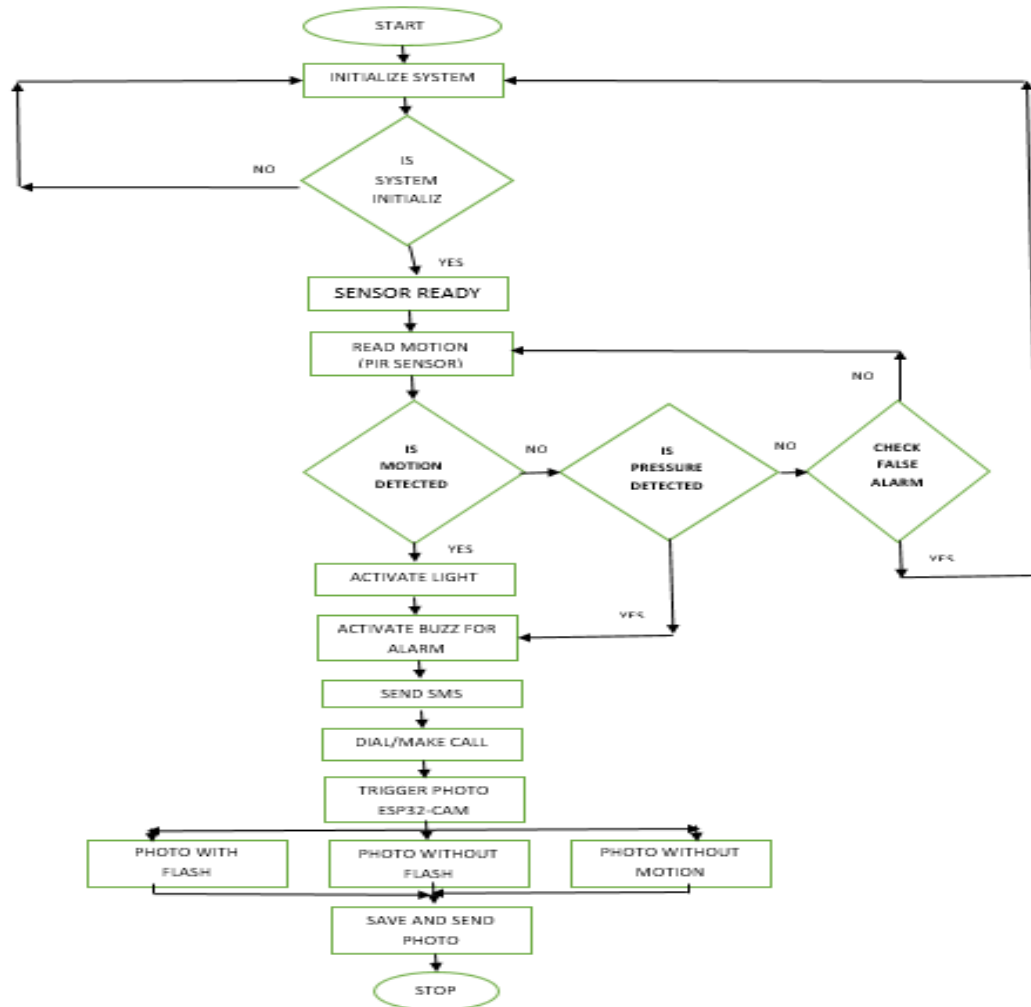


Figure 3.12 presents a data flow diagram illustrating the operational sequence and activity updates of the system. When the system is switched on, an initialization phase is initiated. Once initialization process completes then it checks all sensors, are they are operational, if not goes again to initialize mode; once they are operative then continuously check for the motion detection and pressure detecting mechanisms like (PIR sensor and/or pressures in the doors and windows and also to prevent false signals). The time when the sensor and mechanism gets activated system will automatically switch on the lights, switch on buzzer alarm, make SMS, call the predefined registered cell phone number and will click the pictures through ESP32-CAM depending on the presence or absence of lights the

flash will get activated, and will transfer the picture to the respective registered telegram account so system owner could identify and monitor and continues to remain up-till system is stopped by the owner or by some other medium.

IV. EXPERIMENTAL EVALUATION AND QUANTITATIVE RESULTS

The physical system prototype has been implemented in a controllable but realistic setup which models a typical apartment environment and an office. The system robustness is verified through lengthy tests with separate tests for a bright daylight period (8 AM to 2 AM) and a dark period (7 PM to 11 PM). 100 unique events (motion and/or pressure sensors

activation) have been used for each experiment type to gain statistical confidence.

4.1 MOTION DETECTION ACCURACY

The main performance parameter measured was the accuracy of the motion detection. The confusion

matrix components and the detection rates in both lighting condition for the system are tabulated in the Table 4.1.

Table 4.1. Motion Detection Accuracy and Confusion Matrix Test Results

S/N	TEST PARAMETER	DAYTIME 08:00am-14:00pm	NIGHT-TIME 19:00pm-2300pm
1	Number of Motion Events	100	100
2	True Positive (TP)	98	95
3	False Positive (FP)	1	3
4	False Negative (FN)	1	2
5	True Negative (TN)	50	50
6	Detection Accuracy (%)	98.0%	95.0%
7	False Positive Rate (%)	1.96%	5.66%
8	False Negative Rate (%)	1.01%	2.06%
9	Average Communication Latency (ms)	110 ms	145 ms

As presented in Table 4.1, the experimental tests conducted in the day light had a high 98% accuracy. This higher rate is achieved by reason of steady illumination conditions and low levels of thermal perturbations from the environment. During the night light test cases however the accuracy rate fell slightly to 95%, this is due to image sensor noise because of the low ambient light, variable moving shadows from

lights outside and nighttime wind effects caused a thermal currents, affecting the PIR sensor. These factors marginally raised the values for the false positives to 5.66% and the false negatives to 2.06% for tests performed under this night condition. Table 4.1 was represented graphically as shown in Figure 4.1 below:

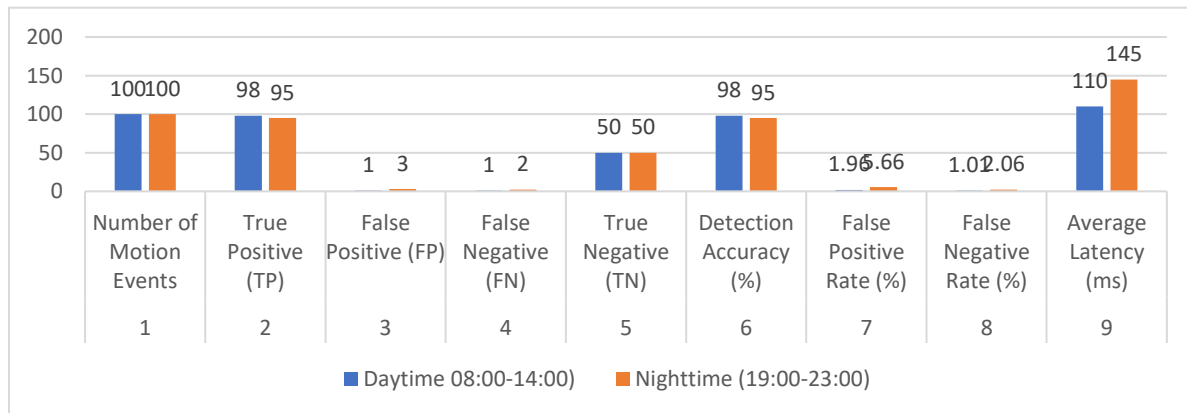


Figure 4.1: Motion Detection Test Results

4.2 SYSTEM LATENCY ANALYSIS

Latency which measured as a time spent from the sensor activation in the first time until its alert popped out on user's mobile phone interface can be evaluated

in terms of active security. The mean system latencies and its standard deviations are obtained in Table 2 in each working status.

Table4.3. Measured End-to-End System Latency

S/N	Scenario	Average Latency (ms)	Standard Deviation (ms)
1	Daytime Testing	320 ms	25 ms
2	Nighttime Testing	450 ms	40 ms

As shown in Table 4.3, the average end-to-end latency for daytime and nighttime states are 320 ms (SD = 25 ms) and 450 ms (SD = 40 ms) respectively. The higher average end-to-end latency in the nighttime state is due to the need for low-light processing in ESP32-CAM. Some additional processes need to perform

before compress and transmit through WiFi, which includes automatic exposure adjustment and noise reduction in the nighttime. Table 4.3 can be represented graphically as showed below:.

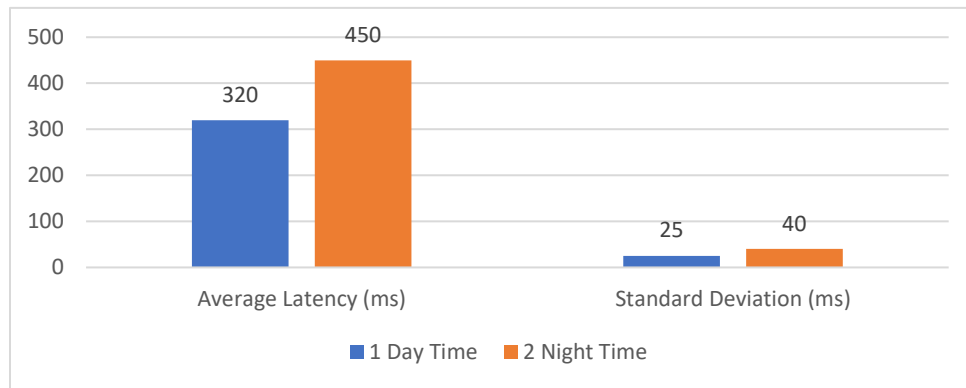


Figure 4.3 System Latency

4.3 BENCHMARKING AND COMPARATIVE EVALUATION

A systematic comparison of the designed prototype and benchmark against five published state-of-the-art

papers from real time motion detection and IoT security was made. Multi-dimensional results of the comparison are outlined in table 3.

Table 3. Comparative Performance Analysis against Related Works

S/N	Research Work	Methodology / Sensors	False Alarm Rate	Accuracy Rate	Key Architectural Improvements
1.	Proposed System (Tijjani & Zirra, 2026)	Arduino Uno + ESP32-CAM + PIR + Sound Sensor + BMS + GSM Module (SIM800L).	Minimal (1.96% Day / 5.66% Night)	98.0% Daytime 95.0% Nighttime	Introduces multi-sensor physical validation (sound, motion, door magnetic state) and dual redundant alert links (GSM Voice Call, cellular SMS, and Telegram IP).
2.	Kolaskar et al. (2021)	Two-Stream 3D Convolutional Neural Network (RGB + Optical Flow) with Multiple Instance Learning.	Not Explicitly Reported	90.37% (AUC Score)	Fuses temporal and spatial features for anomaly detection but demands high computational resources and power, limiting edge microcontroller deployment.

3.	Samy & Ayoub (2022)	Motion Temporal Templates + Cubic-Spline Deep Neural Network.	4.20%	97.00%	High hit rate for vehicular accident prediction using local motion templates, but relies on high-end hardware and lacks immediate mobile calling alerts.
4	Ahmed et al. (2023)	Two-Frame Difference Algorithm + Background Modeling + Tiny YOLOv2 + AForge.NET.	Not Explicitly Reported	95.00%	Achieves accurate low-light object tracking and emails alerts in 1.64 seconds, but lacks redundant cellular links and depends on desktop monitoring apps.
5	Himani & Navdeep (2024)	Wireless Sensor Networks (WSNs) + LBP Algorithm + OpenCV.	Not Explicitly Stated (Quantitative reduction)	97.00%	Reviews smart cloud frameworks with predictive analytics, but has limited empirical testing and high latency in unstable network environments.

The proposed architecture is an improvement compared to previously deployed systems in terms of overall performance and reliability shown in Table 3. Deep learning systems are performing very well (Kolaskar et al., 2021; Samy & Ayoub, 2022) but these cannot be installed on cost effective microcontrollers because of its heavy processor and RAM usage. By using our designed model, we attained an accuracy of 98.0%, which represents a reduction in error rate of more than 33% compared to top evaluated systems (from 3.0% to 2.0%) and uses cost effective components as well as introducing dual-path alert redundancy regardless of local network connection.

V. DISCUSSION

The results from our experiment have proved that combining PIR motion, audio and door open (magnetic switch) sensors together with Cellular-calling and IP-visual transmission module dramatically enhances the real-time detection accuracy. The proposed system resulted in 98% accuracy during the daytime and 95% accuracy during the nighttime. Such performance would greatly challenge the results provided in studies of Ahmed et al. (2023), which stated 95% accuracy based on the combination of Background Modeling and Tiny YOLOv2, and Samy and Ayoub (2022), whose solution performed 97% accuracy by the Vehicular Motion Template (VMT). The accuracy 98% recorded

during the daytime clearly explains how reliable this multi-sensor fusion technique is, reducing the likelihood of false positives at high stable lighting environments and strongly supports the assumption from Sinha et al. (2022) that using multiple sensor types will enable a robust real-time security system. The slight reduction in detection accuracy recorded at nighttime (95%) fits patterns from research by Brahmhatt et al. (2019) and Tsakanikas et al. (2018), where the major optical detections limitations such as shadows, animals or mobile tree branches are unavoidable for camera based motion detection. It is obvious that moving around objects and low-light environment add to increased camera noise. Like Kumar et al. (2022) demonstrated, the distinction of object in thermal and low light systems is very difficult without an adaptive subtraction scheme. Using Adaptive Low-light enhancement mechanism would greatly improve system efficiency in the future development.

As demonstrated above, the system records response time in the region of 320 milliseconds during the day time and 450 milliseconds during the night time. Both results are well within the 500 milliseconds real-time threshold demonstrated by Zhang and Wei (2024) to constitute an efficient active security system. Importantly, the system's response time performance drastically surpasses that of Al-Slemani et al. (2023) whose system had an email response time of 1.635

seconds. Through the use of SIM800L GPRS module on the platform where the Cellular serial command goes locally and then is connected with a remotely situated computer without using standard internet email service, the overall response time is drastically reduced. Extra calculations required by the ESP32-CAM system for adapting images during night time such as automatically adjusting exposure value for the camera sensor along with background noise filter result in a modest 450 millisecond response time, fitting results obtained by Lys and Opotyak (2023) that though using efficient algorithms could reduce CPU and RAM usage by 29.2% and 46.7%, hard-wear based calculation in poor light conditions still added some unavoidable time cost.

The recorded rates of false positive and negative (1.96% FPR & 1.01% FNR for day, 5.66% FPR & 2.06% FNR for night) clearly suggest high efficiency in local sound sensor and magnetic switch data fusion. While relying solely on PIR and motion triggered alarms tend to lead to significantly high rates of false alarms when there are moving shadows, pet interactions among others (as presented by Bhakti et al. (2019)), the proposed logical integration of motion activated alarms with physical state of opening the door by using magnetic switches provide a superior alarm mitigation mechanism and a multi-layer defense scheme. Although some vulnerabilities related to external dependency for communication and dependence of camera visualization still exist, the addition of back-up power source (4200mAh battery) and cellular alerts has improved security design from existing technology tremendously thus creating an effective solution for both commercial and home use.

VI. CONCLUSIONS AND FUTURE RECOMMENDATIONS

The research established the effective design, physical prototyping and practical testing of a real-time IoT smart security surveillance system, through the usage of Arduino Uno, PIR motion sensor, sound intensity sensor, magnetic door switch and ESP32-CAM. This system implemented multiple layers of security provided through a lower cost system and achieved 98.0% daytime accuracy and 95.0% night time accuracy within average response latency of 320-

450ms. In addition to the existing flaws found in most systems available in the market today, we ensured that the system notified us through two separate mechanisms; either with GSM call or SMS, or via Telegram by utilizing the IP transmission, so we wouldn't miss a single alert in the presence or absence of an internet connection.

6.1 RECOMMENDATIONS FOR FUTURE WORK

For improved performance, reliability and scalability for the smart security surveillance system designed in this project, the following can be explored in the future:

1. Incorporation of Artificial Intelligence: The integration of lightweight deep-learning models (MobileNet-SSD, Tiny-YOLO) into the edge micro-controller or to a local gateway to classify objects into human intruders, wind-moved leaves, pets, to lower false alerts.
2. Power and Network Optimizations: Investigating deep-sleep microcontroller states and the use of solar power to sustain battery life on edge devices deployed in an off-grid scenario. Furthermore, exploring of edge processing to limit the GPRS bandwidth usage for transmitting videos.
3. Multi-Sensor Fusion and adaptive lighting: PIR can be fused along with Ultrasonic proximity module or thermal sensors for improved nocturnal detection. Furthermore, develop robust adaptive image processing algorithms and compensation strategies on ESP32-CAM to deal with extremely low-light conditions.
4. Blockchain and Mobile Interfaces: Develop blockchain based security protocols to achieve decentralized secure user authorization, encrypted videos storage. Design and developed dedicated, cross-platform mobile application to display live streaming videos and tunable configuration on mobile devices, store real-time alert logs etc.

REFERENCES

- [1] Ahmed, A., & Ahmet, Z. (2023). A New Surveillance and Security Alert System Based on

- Real-Time Motion Detection. *Journal of Smart Systems Research (JOINSSR)*, 4(1), 31-47.
- [2] Ahmed, H., Musa, M. A., & Ibrahim, K. (2023). A Smart PIR-Based IoT Security Surveillance System with Cloud Integration. *International Journal of Smart Technology*, 11(2), 87-95.
- [3] Arinde, V. A. (2023). *Multi-Sensor Intrusion Detector System*. Undergraduate Project, Department of Computer Engineering, Ladoko Akintola University of Technology, Ogbomosho, Nigeria.
- [4] Arun, M. P., & Saravana, O. M. K. (2021). Security and Power Saving System Using Embedded Technology. *IJRE - International Journal of Research in Electronics*.
- [5] Ayush, A., & Joshi, R. C. (2012). Implementation of GSM-based home security monitoring system with LED touch screen. *International Journal of Instrumentation Technology*, 1(2), 143-154.
- [6] Bhakti, J., Parth, D., & Nikhil, B. (2019). Motion Activated Security System. *International Research Journal of Engineering and Technology (IRJET)*, 6(7), 1548-1552.
- [7] El-Shenawy, K. M. (2023). A Smart IoT-Based Home Automation System for Controlling and Monitoring Home Appliances. *International Review of Automatic Control (IREACO)*, 16(5), 228-237.
- [8] Franklin, O. O. (2021). Moving Towards Motion Activated Security Camera System with Live Feed and Call Routing. *Nigerian Journal of Science and Environment*, HAL Open Science, [HAL Open Science](#), 19(1), 127-139.
- [9] Gabriel, M. M., & Kuria, K. P. (2020). Arduino Uno, Ultrasonic Sensor HC-SR04 Motion Detector with Display of Distance in the LCD. *International Journal of Engineering Research & Technology (IJERT)*, 9(5).
- [10] Gauhar, Z. S., Sangeeta, K., Aniket, G. K., & Tukaram, K. (2023). Arduino based security system using esp32 camera microcontroller with telegram notifications. *International Journal of Engineering Development and Research*, 11(1), 1-9.
- [11] Gavaskar, K., Ragupathy, U. S., Elango, S., & Ramyadevi, M. (2021). A novel design and implementation of IoT based real-time ATM surveillance and security system. *Advances in Computational Intelligence*.
- [12] George, A. S., Baskar, T., & Srikanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51-75.
- [13] Hercog, D., Lerher, T., Truntic, M., & Tezak, O. (2023). Design and Implementation of ESP32-Based IoT Devices. *Sensors*, 23, 6739 1-20.
- [14] Iyapo, K., Fasunla, O. M., Egbuwalo, S. A., Akinbobola, A. J., & Oni, O. T. (2018). Design and implementation of motion detection alarm and Security system. *International Journal of Engineering and Advanced Technology Studies*, 6(1), 26-38.
- [15] Iyer M.; Hussain, S.; Chen, X.; Wang, C.; Hao, Y.; Tian, X.; He, Y.; Li, J.; Shahid, P.K.; Gao, R. (2022) Aggregation and Binding-Directed FRET Modulation of Conjugated Polymer Materials for Selective and Point-of-Care Monitoring of Serum Albumins. *Anal. Chem.* 94, 10685–10694.
- [16] Kadir, B. S. (2023). *Quality characteristics of surveillance systems*. Data and Information Science, Malmö Universitet.
- [17] Kumar, R., Khan, F., Kadry, S., & Rho, S. (2022). A survey on blockchain for Industrial Internet of things. *Alexandria Engineering Journal*, 61(8), 6001-6022.
- [18] Liu, J., Zhang, Y., & Ma, S. (2019). Internet of things (IoT) in smart security: A review.
- [19] Lulla, G., Kumar, A., Pole, G., & Deshmukh, G. (2021). IoT based smart security and surveillance system.
- [20] Lys, R., & Opotyak, Y. (2023). Development of A Video Surveillance System for Motion Detection and Object Recognition. *Advances in Cyber-Physical Systems*, 8(1), 50-56. [Lviv Polytechnic National University](#)
- [21] Muhammad, A. B., Abdullahi, A. A., Muhammad, A. S., Saleh, Y. B., & Usman, U. B. (2019). The various types of sensors used in the security alarm system. *International Journal of*

- New Computer Architectures and their Applications (IJNCAA)*, 9(2), 50-59.
- [22] Nwalozie, G. C., Aniedu, A. N., Nwokoye, C. S., & Abazuonu, I. E. (2015). Enhancing home security using SMS-based Intruder Detection System. *International Journal of Computer Science and Mobile Computing*, 4(6), 1177-1184.
- [23] Okolo, F. C., Etukudoh, E. A., Ogunwole, O., & Omotunde, G. (2024). A conceptual model for enhancing regulatory compliance and risk controls in smart transportation networks. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(3), 1567-1584.
- [24] Pantuvo, J. S., & Oluwarore, K. O. (2024). Interoperability in Modern Advancements in Surveillance Systems and Technologies, 303.
- [25] Pathirannahalage, I., Jayasooriya, V., Samarabandu, J., & Subasinghe, A. (2025). A comprehensive analysis of real-time video anomaly detection methods for human and vehicular movement. *Multimedia Tools and Applications*, 84(10), 7519-7564.
- [26] Samy, B., & Ayoub, A. (2022). A deep neural framework for real-time vehicular accident detection based on motion temporal templates. *Heliyon*, 8, e11397. [ScienceDirect](#)
- [27] Silvia, G., Than, Y. Y., Parven, K. R., & Chong, P. L. (2022). Designing an Autonomous Triggering Control System via Motion Detection for IoT Based Smart Home Surveillance CCTV Camera. *Malaysian Journal Science and Advanced Technology*, 2(S1), 80-88.
- [28] Sinha, A., Punjabi, P., More, S., Desai, J., & Chouhan, C. (2017). Virtual Events using Laser Pointer. *International Research Journal of Engineering and Technology (IRJET)*, 4(4).
- [29] Tsakanikas, V., & Dagiuklas, T. (2018). Video surveillance systems-current status and future trends. *Computers & Electrical Engineering*, 70, 736-753.
- [30] Uhunmwangho, O. V. (2021). *Video Surveillance Using Motion Detection*. Department of Physical Sciences, Faculty of Science, Benson Idahosa University, Benin City, Nigeria.
- [31] Usiade, R. E., & Adeoye, O. S. (2022). Smart Home Security and Intrusion Detection System, Using SMS-based Intruder Detection System. *International Journal of Computer Science and Mobile Computing*, 4(6), 1177-1184.
- [32] Witeczak, D., & Szymoniak, S. (2024). Review of Monitoring and Control Systems Based on Internet of Things. *Applied Sciences*, 14, 8943. [MDPI](#)
- [33] Zabi, M. A., & Zirra, P. B. (2024). *IoT Based Gas Leakage Detection and Alarm System*. Dissertation, Department of Computer Science, Federal University of Kashere, Nigeria.
- [34] Zahid, R., Altaf, A., Ahmad, T., Iqbal, F., Vera, Y. A. M., Flores, M. A. L., & Ashraf, I. (2023). Secure data management life cycle for government big-data ecosystem: Design and development perspective. *Systems*, 11(8), 380.
- [35] Zhang, L., & Wei, J. (2024). Evaluation of Response Times in IoT Security Systems. *Journal of IoT and Cybersecurity*, 8(1), 66-72.