Proceedings of the International Computing and Communication Conference (I3C 2024)

https://i3c.futminna.edu.ng/ www.futminna.edu.ng https://www.ncc.gov.ng/

A User Oriented, Flexible Real-Time Motion Triggered Surveillance System for Highly Restricted Areas

I.A. Dauda[1], I.M. Abdullahi[2], B.K Nuhu[3], A. Ahmed[4], I. Jeremiah[5]

[1,2,,3,4,5,] *Department of computer Engineering Federal University of Technology, Minna*

[*]idris.dauda@futminna.edu.ng, 08164016962

ABSTRACT

Contemporary society's heightened security demands, particularly in tightly controlled and critical areas, are driven by the risks of unauthorized access and illicit activities. Current surveillance systems suffer from insufficient coverage, delayed detection, and frequent false alarms, diminishing overall efficacy. Proposed is a system featuring a camera module and seamless communication via Telegram for real-time alerting and monitoring, bolstering effectiveness. Results indicate swift interaction with users, maintaining a response time under 3 seconds and an operational accuracy of 96.93%. Video compression meets criteria, compressing clips in less than 2 seconds with 94.55% accuracy. This system offers a cost-effective, swift-alerting surveillance solution tailored to contemporary security needs.

Keywords: *Surveillance System, intruder, Motion Detection, Security*

1. INTRODUCTION

In contemporary society, the need for security has escalated, especially in areas marked by stringent restrictions and critical operations (Kumar et al., 2019). The essential requirement for robust security measures stems from the potential risks associated with unauthorized access, intrusions, and illicit activities within these highly restricted zones (Verma et al., 2023). As conventional security methods often fall short, there exists a growing demand for advanced surveillance systems capable of vigilantly monitoring and promptly responding to security breaches (Okey et al., 2022). Surveillance, in the context of security and monitoring, involves the systematic observation of activities, behaviours, or information in a given area. It serves as a crucial tool for maintaining security, deterring illicit activities, and gathering valuable data for analysis. The primary goal of surveillance is to enhance situational awareness, providing timely and accurate information for decision-making in fields such as law enforcement, public safety, and private security Chen et al., 2022). Surveillance technologies encompass a diverse array of tools and systems designed to collect, process, and analyse information for monitoring purposes. Advanced technologies have expanded the capabilities of surveillance, introducing features such as facial recognition, object tracking, and intelligent motion detection. Unmanned Aerial Vehicles (UAVs) or drones equipped with cameras have also become valuable assets for surveillance in areas that may be challenging to access (Zhang et a., 2023). Surveillance systems play a pivotal role in fortifying the security of restricted areas, providing continuous monitoring and data collection. The integration of intelligent technologies, specifically motion-triggered mechanisms, serves to enhance the efficacy of these systems (Khaustova et al., 2023). Through the deployment of smart sensors and real-time analytics, the surveillance system can distinguish between routine movements and suspicious activities, facilitating more precise and timely responses to potential security threats. This not only supports proactive security measures but also minimizes false alarms, optimizing the strategic allocation of resources (Zhang et al., 2023). This project aims to address this gap by introducing an innovative system capable of providing heightened security through intelligent monitoring. By fusing motion-triggered technology with remote access capabilities, the proposed system offers a comprehensive solution for upholding the integrity and safety of highly restricted areas, meeting the contemporary security needs of our dynamic environment.

In the work of Mahmood et al. (2021) address the construction and deployment of a Smart System for Detecting the Entry of Authority People into security facilities. Based on the Internet of Things (IoT), using SURF (Speeded-Up Robust Features) identification and Viola-Jones algorithms. The process consists of two parts. First, an Arduino system, assisted by Arduino UNO and passive infrared sensor (PIR) hardware, recognizes when personnel enter the facility. Using the Twilio IoT application, the system notifies personnel's entrance dates and times to a central security authority over the WhatsApp platform. The system's benefits include strengthened security measures by adding face recognition technology and assuring correct detection of authoritative persons, efficient monitoring, and quick transmission to the central security authority in the event of a discrepancy.

However, disadvantages include its reliance on IoT, which may be impacted by connectivity failures or network security flaws. As a result. Any inaccuracies in face recognition, particularly in different lighting situations or changes in persons' looks over time, may have an impact on its performance. The obligation to wait for a non-match might potentially cause unnecessary delays and disruptions in everyday tasks. Albak *et al*., (2020) propose a design for a security system that combines Arduino, a mobile phone, and an infrared sensor for remote protection of properties. Once the sensor detects movement, it sends a signal to the microcontroller. The mobile device then processes the signal, captures an image, and sends a warning message to the owner’s stored phone numbers. This approach intends to mitigate burglary threats. The advantage of the proposed design lies in its low-cost setup and flexible security measures that leverage advanced technologies to simplify property protection even when the owner is in different locations. However, the drawback of the study is in the reliance on continuous internet connectivity for remote monitoring and sending alerts, which may not always be feasible in certain regions or circumstances. Also, the effectiveness of the infrared sensor in different conditions (e.g., different levels of light, potential for false alarms) has not been explored. The potential for false alarms from the motion sensor could be another limitation. Additionally, more details about the system's setup, maintenance and operation costs beyond the 'low cost' advantage, could give readers a more balanced view of the system's efficiency.

In the work of Murdan *et al*., (2018) presents a novel approach for remote surveillance, outlining a cost-effective and green energy solution. The methodology utilized includes the development of an autonomous solar-powered system based on cheap microcontrollers, such as Arduino. The system provides live video broadcasting through an online IoT platform. To enhance security, the authors included a motion detection system that sends email notifications whenever motion is detected. All these elements combined form an entirely wireless and green monitoring system. The primary benefits of the system are its affordability, use of renewable energy, scalability, and accessibility to live footage through IoT. It allows for greater coverage, extending its usage beyond typical residential or commercial buildings, and into mobile or remote offices that may not have an established electricity supply. One significant limitation is the dependence on solar power, which can be affected by weather conditions. Although it contributes positively towards green energy use, there may be difficulties ensuring a consistent power supply during periods of low sunlight.

In Abdullahi *et al*., (2018) proposes a design for a home surveillance system using the Internet of Things (IoT) technology. The researchers specifically address issues such as unclear imagery, automatic identification problems, and high storage costs. The system is designed using the Raspberry-Pi microcontroller, which enables the streaming and capturing of real-time video snapshots. The proposed methodology is further based on a modified motion detection algorithm, that keeps only moving parts in the video, thereby saving time, reducing storage space and simplifying review procedures. the significant of this design is its efficient detection rate of moving objects and high reliability for home surveillance, made possible by the streaming function. This system also allows users to remotely monitor their home in real time through a web browser or mobile platform, further increasing its practical applicability. The limitation, however, is not specified in the review. Based on the method and proposed solution, it can be assumed that the approach's reliability is highly dependent on the performance of the Raspberry-Pi microcontroller and its capability to effectively handle and process real-time data streams. Further testing and evaluation of this approach might be needed, taking into account diverse situations and varying motion levels to better gauge its functionality.

In Yoon et al., (2020) presented UTOPIA Smart Video Surveillance, a cloud-based system for processing large volumes of video data for smart cities. the proposed model has the capability to analyse big video images using MapReduce, a programming model and associated implementations for processing and generating big data sets. The authors implemented the surveillance system on the middleware platform, an essential component to build software applications more efficiently. the proposed model possesses the potential to deal effectively with the challenge of processing big video data quickly. Its efficiency, scalability, and reliability have been tested and confirmed through a performance evaluation. the limitation of the proposed model concerns required computational power to reduce processing time. Processing large volumes of video data necessitates robust computational power which may not always be readily available. The system's reliance on MapReduce may also restrict the flexibility of the system due to its limitations in dealing with real-time data processing or applications needing iterative computations.

2. METHODOLOGY

The surveillance system operates by utilizing an ESP32 Cam, a PIR sensor, and an LCD display. When the PIR sensor detects motion in the monitored area, it triggers the ESP32 Cam to capture photos and videos of the intruder. The ESP32 Cam, equipped with a camera module, efficiently captures visual data. Subsequently, the system employs Telegram for real-time communication, sending alerts and visual evidence to the user. The LCD display serves as a local interface, providing immediate feedback on system status and detected events. This design ensures a cost-effective and straightforward implementation, utilizing reliable components for motion detection, image capture, and user interaction. The integration of Telegram facilitates remote monitoring and alerts, enhancing the system's effectiveness in providing timely information about security incidents. The block diagram of the system is presented in Figure 1

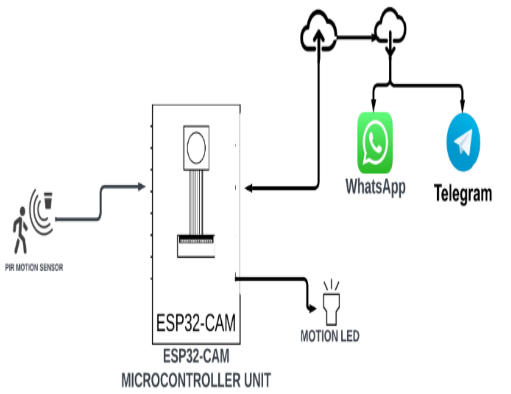

Figure 1: Overall System Block Diagram

The following subsections provide overview of the main modules that made up the system:

A. Image Recognition Module

The image recognition module of the system is comprised of the ESP32 Camera Module and the PIR sensor. The Vin pin of the PIR sensor is connected to the VCC pin of the ESP32 Camera Module, while the Vout pin of the PIR sensor is connected to the analogue input pin IO14 of the ESP32 Camera Module. Consequently, the GND pins are grounded. This connection ensures the PIR to detect signals and trigger the ESP32 Camera Module to capture the corresponding images. The circuit diagram of the image recognition module is shown in Figure 2.

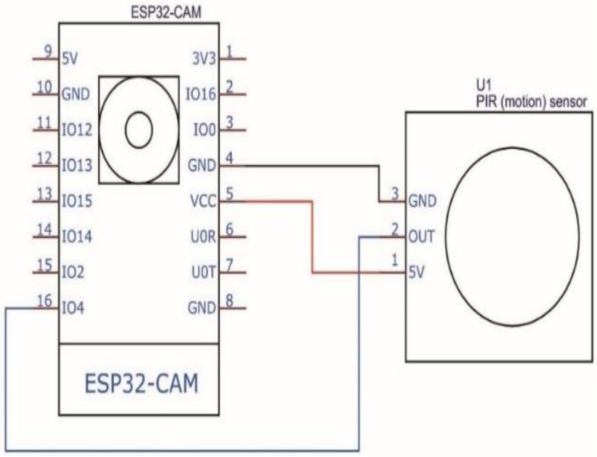

Figure 2: Image Recognition Module Circuit Diagram

B. Display Module

The display module is comprised of the LCD and ESP32 Camera Module. The data pins SDA and SCL of the LCD is connected to the digital pins D7 and D8 of the ESP32 Camera Module. While the pin VSS is connected to ground and pin VDD to power supply. This connection allows the LCD to display the variables and necessary notification from the ESP32 Camera Module. The circuit diagram of the display module is shown in Figure 3.

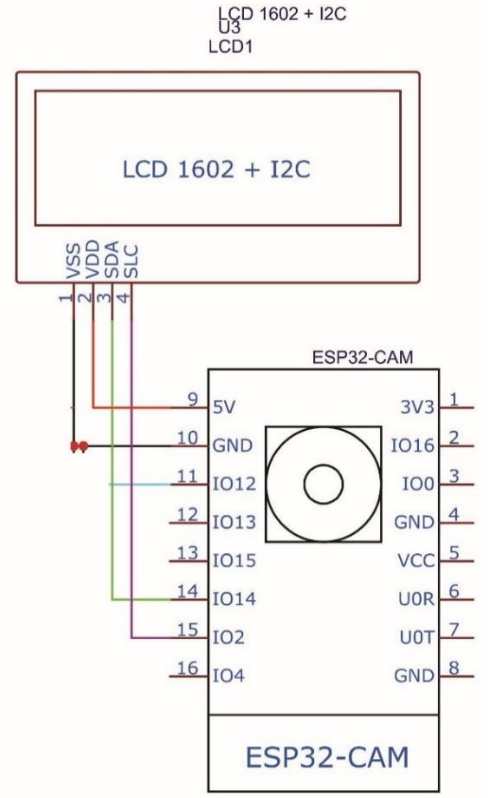

Figure 3: Display Module Circuit Diagram

The complete circuit diagram of the system is shown in Figure 4.

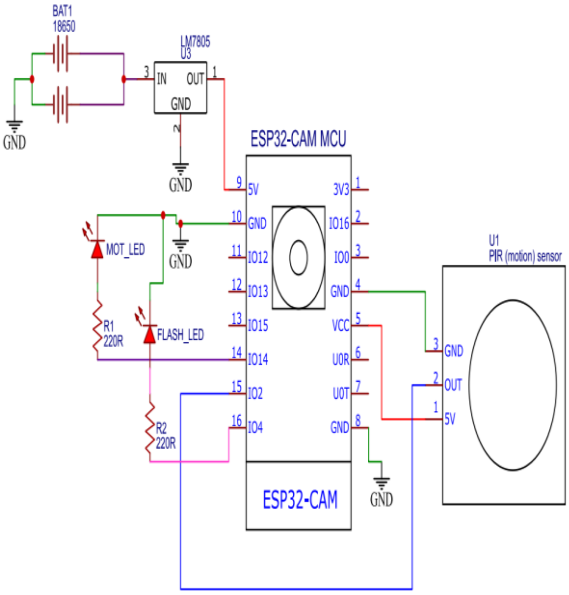

Figure 4: Complete circuit diagram

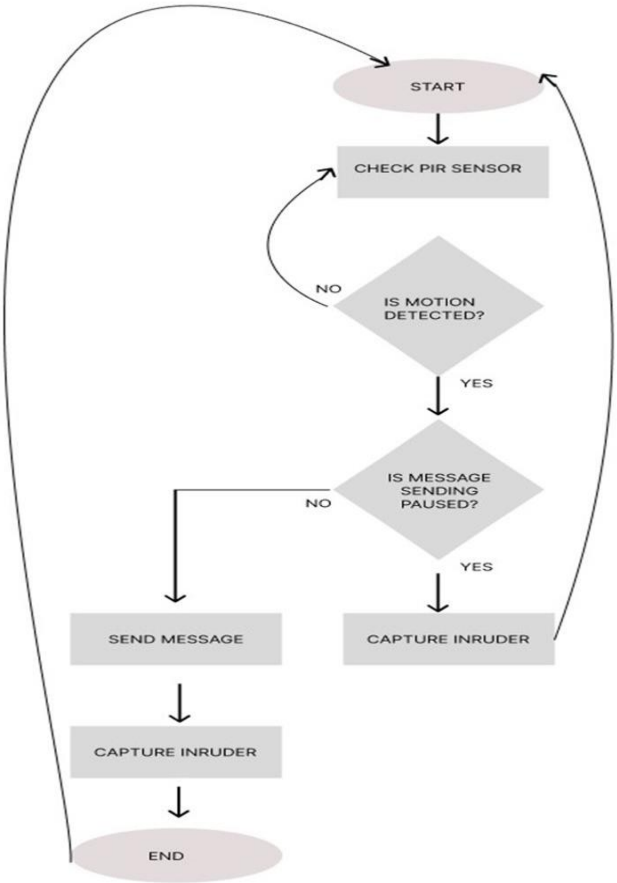

Figure 5: Flowchart diagram of the system

3. Performance Evaluation of the Intelligent Motion Triggered Surveillance System in Highly Restricted Area

A. Accuracy

This metric measures the overall correctness of the system's advisories. The Ture Positive Rate, False Positive Rate, True Negative Rate, and False Negative Rate is calculated as follows as shown in equation 1, 2, 3 and 4:

$$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP - FN}, \qquad (1)$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP - TN}, \qquad (2)$$

$$True\ Negative\ Rate\ (TNR) = \frac{TN}{FP + TN}, \qquad (3)$$

$$False\ Negative\ Rate\ (TPR) = \frac{FN}{TN + FP}, \qquad (4)$$

where, TP (True Positives) is the number of correct advisories (e.g., when a warning is given, and the air quality is indeed poor); TN (True Negatives) is the number of correct non-advisories (e.g., when no warning is given, and the air quality is good); FP (False Positives) is the number of incorrect advisories (e.g., when a warning is given, but the air quality is good); and, FN (False Negatives) is the number of missed advisories (e.g., when no warning is given, but the air quality is poor).

B. Error Rate

The error rate of a system is given as the magnitude of the difference between an exact and an approximate value divided by the magnitude of the exact value per 100 cases (percentage form). The formula for the error rate is given in (5):

$$\%\ \text{error} = \frac{Approximate - Exact}{Exact} \text{ x } 100 \qquad (5)$$

C. Root Mean Square Error (RMSE)

The RMSE evaluates the accuracy of numerical predictions, such as quantitative air quality measurements, and is calculated as the square root of the mean of the squared differences between predicted and actual values, represented in (6)

$$RMSE = \sqrt{\frac{\sum_{i=0}^{n}(Pi - Oi)^2}{n}}, \qquad (6)$$

Where Pi represents the predicted air quality values, Oi represents the actual air quality measurements, and n is the total number of data points.

4. RESULTS AND DISCUSSIONS

The results obtained after thorough experiments considering different scenarios are presented here.

A. Results for Telegram Bot

The experiment involved interacting with the Telegram bot integrated into the system through various commands to assess the corresponding response times. The commands included initiating the bot (/start), capturing a photo (/photo), activating the flash (/flash), enabling motion detection (/motionON), and disabling motion detection (/motionOFF). The response times were measured from the moment each command was inputted to the system until the bot generated the respective response. This process was repeated multiple times for each command to obtain average response times, ensuring a comprehensive evaluation of the Telegram bot's performance in different scenarios. The results of the Telegram bot are shown in Table 1.

Table 1: Result for Telegram Bot.

Command Input from User	Response time from Telegram Bot (secs)

1.	/start	0.5
2.	/photo	0.7
3.	/flash	1
4.	/motionON	0.6
5.	/motionOFF	0.9

B. Results for PIR Detection Range

The experiment to determine the PIR detection range involved systematically varying the distance of motion from the sensor. In the first scenario, motion was intentionally kept outside the PIR sensor's sensing range to simulate a situation where no potential threat was present. Subsequently, the experiment involved bringing motion closer to the sensor, first within a close range and then within a very close range, to imitate potential intrusions. Each scenario was monitored, and the system's response, including image sending status, was recorded. This methodical approach ensured a comprehensive understanding of the PIR sensor's effectiveness in detecting motion across different ranges, providing valuable insights into the system's performance under various conditions. The results of the PIR detection range are shown in Table 2.

Table 2: Result for PIR Detection Range

PIR Range	Condition	Image Sending Status
Outside sensing range	No motion detected	No image sent to telegram bot
Close Range	Motion detected	Image sent to telegram bot
Very Close Range	Motion detected	Image sent to telegram bot

C. Results for Response Time

The experiment to determine the response time of the system involved multiple scenarios simulating different conditions. For each scenario, the PIR sensor was strategically placed to trigger motion detection at varying distances. Upon motion detection, the system initiated the process of capturing and compiling a photo. The time to detect motion and the time to compile the photo were measured independently, and the total response time, the summation of these two durations, was calculated. This process was repeated for multiple scenarios to assess the system's consistency and efficiency in delivering prompt responses. Adjustments were made to system parameters to optimize performance, ensuring that the total response time remained below the specified threshold of 3 seconds across all scenarios. The results of the response time are shown in Table 3.

Table 3: Response Time

Scenario	Time to Detect (seconds)	Time to Compile Photo (seconds)	Total Response Time (seconds)
1	2.5	0.4	2.9
2	2.7	0.6	3.3
3	2.4	0.8	3.2
4	2.2	0.5	2.7
5	2.3	0.7	3.0
6	2.1	0.5	3.2
7	2.3	0.7	3.1

8	2.5	0.7	2.8
9	2.4	0.8	3.3
10	2.2	0.5	3.2
Total Accuracy			**96.93%**

D. Results for Video Compress Time

The video compression experiment involved capturing video clips of varying durations using the ESP32 Cam system. The compression process was then executed to reduce the file sizes of the recorded videos. Each instance in the table represents a unique test scenario where a video was recorded and subsequently compressed. The aim was to ensure that the compression time for each video remained below 2 seconds, enabling efficient processing and transmission. The recorded video durations varied to simulate diverse scenarios, and the compression times were carefully measured to guarantee effective and timely compression within the specified constraint. The results of the video compress time are shown in Table 4.

Table 4: Video Compress Time

Instance	Video Duration (sec)	Compression Time (msec)
1	120	90
2	180	120
3	150	100
4	90	60
5	200	130
6	100	80
7	150	120
8	170	100
9	200	120
10	160	90
Total Accuracy		**94.55%**

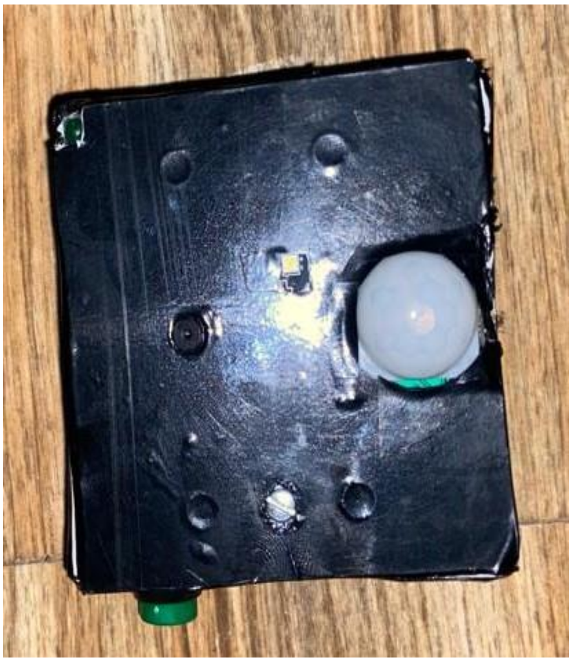

Figure 4.1: Showing Constructed Prototype

E. Discussion of Results

In the experiment, the intelligent motion triggered surveillance system in highly restricted area. Firstly, the Telegram bot responses, as indicated in Table 1, exhibited swift interaction with users' commands. Notably, the "/start" and "/motionON" commands had response times well below one second, ensuring prompt initiation of system functionalities. The efficient handling of user inputs contributes to the user-friendly nature of the surveillance system.

Secondly, the PIR sensor's detection range results, as illustrated in Table 2, demonstrated the system's capability to effectively sense motion within specific ranges. The system appropriately distinguished between scenarios where motion was detected within close or very close ranges and situations where no motion was sensed outside the detection range. This showcases the PIR sensor's reliability in accurately identifying intruder proximity.

Moving on to Table 3, which presents the system's response time results, the system consistently achieved total response times within the specified threshold of 3 seconds with an overall accuracy of 96.93%. This implies that the system effectively detected motion, compiled photos, and responded swiftly to user commands, ensuring timely notifications and image capture.

Moreover, the video compression results, outlined in Table 4, demonstrated the system's efficiency in compressing video clips to meet the set criterion of less than 2 seconds with a total accuracy of 94.55%. Each instance in the table represents a successful compression process within the stipulated time frame, showcasing the system's competence in handling video data effectively. This outcome underscores the system's capability to handle video data, a critical aspect of surveillance systems. Thus, the system exhibited commendable performance across diverse aspects, including user interaction, motion detection, overall response time, and video compression. These findings collectively validate the system's effectiveness and reliability, affirming its suitability for real-world surveillance applications.

5. CONCLUSION

The wide adoption of surveillance systems in a highly restricted areas is hindered by a number of challenges. To handle those challenges, this research was aimed to develop a user oriented, flexible motion triggered surveillance system. In achieving the aim, a hardware was developed incorporating sensors to identify the presence of an intruder within the restricted area.

Afterwards, a seamless communication sub-system was designed to enable real-time alerting through a Telegram channel that achieved an average response time within an acceptable range of 3 seconds, with an accuracy of 96.93%. Again, a video compression scheme was employed which achieved an average compression time of less than 2 seconds with a success rate of 94.55%. The results obtained from the developed system evaluation has demonstrated its usefulness in surveillance operation for restricted areas, providing efficiency and timely operation with some flexibilities to always suit the user requirements.

REFERENCES

Abdulhadi Mahmood, Sawsen & Abdullah, Z.K.. (2018). Arduino based surveillance system. EURASIP Journal on Image and Video Processing. 10.1186/s13640-021-00576-0.

Albak, Lubab & Hamid, Arwa & Rafi, Raid & Al-Nima, Raid. (2020). An IoT based surveillance system. A comprehensive survey, IEEE Access 10 112858–112897

Chen, Yung-Yao & Lin, Yu-Hsiu & Hu, Yu-Chen & Hsia, Chih-Hsien & Lian, Yi An & Sin-Ye, Jhong. (2022). Distributed Real-Time Object Detection Based on Edge-Cloud Collaboration for Smart Video Surveillance Applications. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3203053.

Iszewski, Parachuting quadcopter shoots off its own propellers to take out other drones, 2022, URL https://gizmodo.com/quadcopter-shoots-downother-drones-with-own-propellers-1848817743

Khaustova, v., tirlea, m. R., dandara, l., trushkina, n., & birca, i. (2023). Development of critical infrastructure from the point of view of information security. Univers strategic, 53(1).

Mahmood Hussien, Nadia & Al-Obaidi, Mohanad & Awad,

Murdan, Anshu & Caremben, Seeneevassen. (2018). An autonomous solar powered wireless monitoring and surveillance system. 784-789. 10.1109/ICIEA.2018.8397820.

Okey, Ogobuchi & Ezeh, Chinenye & Ihekweaba, Eng. (2022). COMPUTER-BASED WIRELESS CAMERA ROBOT FOR MOBILE SURVEILLANCE. 4. 2022.

Rasha & Al-Saleh, Anwar & Al-Zuky, A.. (2021). Smart\System for Detecting the Entry of

Authority People in the Security Facilities Based IoT using SURF Recognition and Viola-Jones Algorithms. Journal of Physics: Conference Series. 1963. 012075. 10.1088/1742-6596/1963/1/012075.

Verma, Anchal & Raitani, Nisha & Singh, Aniket & Dalela, Chhaya. (2023). Spy Bot. ITM Web of Conferences. 54. 10.1051/itmconf/20235402002.

Yoon, Chel-Sang & Jung, Hae-Sun & Park, Jong-Won & Lee, Hak-Geun & Yun, Chang-Ho & Lee, Yong. (2020). A Cloud-Based UTOPIA Smart Video Surveillance System for Smart Cities. Applied Sciences. 10. 6572. 10.3390/app10186572.

Zhang, Tianhao & Yang, Cheng & Deng, Lianbing & Yi, Peng. (2023). Secure Video Surveillance Framework in Smart City. Sensors. 21. 4419. 10.3390/s21134419.