IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

Anti-Drone System

Prof. Dnyaneshwar S. Rajnor, Anjali Patil, Tejas Lodaya, Aayush Jain, Prerana Gangurde
Department of Computer Engineering
SNJB's Late Sau. K. B. Jain College of Engineering, Chandwad, Nashik, India

Abstract: *The "Anti-Drone System" project aims to design, develop, and implement a comprehensive solution for detecting, tracking, and mitigating unauthorized drone activity. As the use of drones becomes increasingly prevalent in various sectors, there is a growing need to address the security and privacy concerns associated with their misuse. This project focuses on the creation of a multi-faceted system that combines cuttingedge technologies such as radar, radio frequency (RF) analysis, and optical sensors to identify and respond to drones effectively. The system will provide real-time monitoring and alerts, enablingrapid response to potential threats. With a strong emphasis on both hardware and software integration, this project strives to offer a reliable, cost-effective, and scalable solution to protect critical infrastructure, public events, and private property from unauthorized drone incursions*

Keywords: Detecting, Tracking, and Mitigating unauthorized drone activity, Image Processing, Reliable, Cost-effective, and Scalable solution.

I. INTRODUCTION

In an age characterized by the widespread presence of drones, the urgency of establishing robust countermeasures to protect security and privacy has never been more pronounced. The subject of this report, the "Anti-Drone System" project, represents a groundbreaking initiative in the field of security technology. This comprehensive system has been meticulouslycrafted to tackle the increasing challenges posed by unauthorized drones, offering a multifaceted approach encompassing detection, image analysis, and the use of laser technology for neutralization.

Drones, once considered innovative tools with a wide rangeof applications, have transformed into powerful instruments for both legitimate and malicious purposes. The availabilityof consumer drones has made it easier for individuals with various intentions to operate these devices, necessitating acomprehensive defense mechanism. The core of this project lies in its three primary functions:

Detection: The system is equipped with state-of-the-art radar, radio frequency (RF) scanning, and optical sensors that work together to rapidly identify and categorize potential dronethreats. This detection capability is crucial for providing realtime awareness of unauthorized drones within its operational range.

Image Processing: Advanced image processing algorithms have been incorporated to analyze incoming drone data. This feature provides valuable insights into the type,size, and flight path of intruding drones, enhancing situational awareness and enabling a more precise response to security threats.

Neutralization through Laser Technology: A standout aspect of this system is its non-lethal neutralization capability. It employs precise laser technology to disable drones in-flight, ensuring a controlled and non-destructive response to security threats while minimizing collateral damage.

The "Anti-Drone System" project, outlined in this report, establishes a new benchmark in comprehensive mitigation of drone threats. Its seamless integration of detection, image processing, and laser-based neutralization reflects a commitment to addressing security and privacy concerns in an era where challenges related to drones are increasingly prevalent. This report aims to provide an in-depth account of the design,development, and operational effectiveness of this pioneering technology, while also considering the ethical, legal, and futureimplications. As we delve deeper into this project, we explore how it addresses critical concerns and ensures a balanced response to unauthorized drone use in today's technological landscape.

II. LITERATURE SURVEY

A preliminary survey is more appropriate than a literature survey for the Anti-Drone system because our system is entirely tailored to the specific needs of the Indian armed forces and complies with the drone security regulations set

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

forth by India's Directorate General of Civil Aviation (DGCA). These regulations, detailed in India's Civil Aviation Requirements (CAR) for drones, were introduced on August 27, 2018, and became effective on December 1, 2018. These are some of thegeneral norms derived from these documents:

All drones, with the exception of those in the Nano category, must undergo registration and be assigned a Unique Identification Number (UIN).

Commercial drone operations require a permit, except for Nano category drones flying below 50 feet and Micro category drones below 200 feet.

Drone operators are obliged to maintain a continuous direct visual line of sight during flights.

Drones are restricted from flying beyond 400 feet in altitude.

Flying drones in designated "No Fly Zones," which encompass areas near airports, international borders, VijayChowk in Delhi, State Secretariat Complex in State Capitals, strategic locations, and military installations, is prohibited.

Authorization for flying in controlled airspace can be secured by submitting a flight plan and obtaining a uniqueAir Defense Clearance (ADC)/Flight Information Center (FIC) number.

The need for an Anti-Drone system arises from the necessityto safeguard critical infrastructure against potential future warfare tactics and to maintain continuous surveillance in border areas close to Indo-Pak, Indo-China, LOC, and LAC. Manned security encounters specific challenges:

- Inadequate 24/7 surveillance.
- Increased demand for manpower.
- Difficulty in countering small drones using traditional methods.

To address these challenges and enhance security in critical areas, this device meets all market requirements and ensures the protection of vital locations from unwarranted surveillance.

Existing system for Anti-Drone System

As per the years passed war fighting strategies also changedtheir tactics war just didn't't limited to the humans,missile andBombs now war is being fought by drones war robots and cyber war.

In year 2022 Russia ukraine taught us many things of being self dependence and also showed us how morden days warfare are and in future if India faces such situation it may me difficult for us to counter these tactics. There are multiple alternative available in market to counter various types ofdrone.

Different Anti-Drone system available in market. They areas follows:

- **Dedrone RF-300 system**: Detects drones through radio frequency emissions, classifies drone types, and provides realtime alerts.
- **Liteye AUDS (Anti-UAV Defense System)**: Detects, tracks, identifies, and mitigates unauthorized drones. Offers multiple countermeasures including jamming and GPS spoofing.
- **Blighter AUDS (Anti-UAV Defence System)**: Provides early warning, tracking, and defeat capabilities against UAVs.It's a modular system that can be integrated into existingsecurity infrastructure.
- **Airbus Dronewatcher**: Provides real-time detection, identification, and tracking of drones. Offers both fixed and mobile configurations.
- **Aaronia AARTOS DDS:** Provides real-time detection, identification, and tracking of drones. Offers both fixed and mobile configurations.
- **Skylock Drone Defender**: Disrupts communication between the drone and its operator. Can force the drone to land orreturn to its starting point.
- **Rafael Drone Dome**: Provides 360-degree, rapid detection and neutralization of multiple drones simultaneously.
- **Elbit Systems ReDrone**: Detects, identifies, tracks, and defeats hostile drones. Offers a variety of countermeasures.
- **Zen Technologies (Indrajaal):**
  It has real time awareness of the situation.
  It has an integrated all current weapons suite and infrastructure.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

It also has a synergistic combination of 9-10 technologies and a 24X7 persistent and autonomous monitoring and tracking service.

Findings from literature survey

- **Diversity in Technology:** Existing Anti-Drone Systems employ a mix of technologies, such as Radio Frequency (RF) sensors, radar, EO/IR cameras, and acoustic sensors, indicating the importance of multi-sensor integration for effective detection and tracking.
- **Range Variation:** The range of these systems varies, with capabilities ranging from 1 km to 10 km. This indicates the need for selecting a system tailored to the specific operational requirements and the size of the area to be protected.
- **Detection and Classification:** These systems are capable of detecting drones through different emissions like RF, and they can classify various drone types. This ability is crucial for understanding the nature of the threat posed by different drones.
- **Countermeasure Capabilities:** Some systems, like Liteye AUDS, offer advanced countermeasures, including jamming and GPS spoofing, providing active defense mechanisms against unauthorized drones.
- **Integration Flexibility:** Blighter AUDS is highlighted for its modularity, allowing integration into existing security infrastructure. This flexibility is valuable for enhancing overall security measures.

III. METHODOLOGY

The methodology of our project goes as follows:
The methodology for countering unauthorized drones in high-security or restricted zones involves a systematic approach combining detection, image processing, and Neutralisation modules.

IV. ANALYSIS TABLE

TABLE I: LITERATURE SURVEY

Sr. No	Existing Anti-Drone Systems	Range	Technology	Features
1	Dedrone RF-300	Up to 1 km	Radio Frequency sensors	Detects drones through radio frequency emissions, classifies drone types, and provides real-time alerts.
2	Liteye AUDS (Anti-UAV Defense System)	Up to 10 km	RF Detection, Radar, EO/IR camera, and Jamming	Detects, tracks, identifies, and mitigates unauthorized drones. Offers multiple countermeasures including jamming and GPS spoofing.
3	Blighter AUDS (Anti-fence System) UAV	Up to 10 km	Radar, RF Direction Find-ing, and EO/IR camera	Provides early warning, tracking, and defeat capabilities against UAVs. It's a modular system that can be integrated into existing security infrastructure.
4	Airbus Dronewatcher	Up to 5 km	RF sensors, Optical Sensors, Acoustic Sensors	Provides real-time detection, identification, and tracking of drones. Offers both fixed and mobile configurations.
5	Aaronia AARTOS DDS	Not specified (depends on configuration)	RF sensors and jamming	Detects and classifies drones based on their RF emissions. Provides options for manual or automatic counter measures

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

6	Skylock DroneDefender	Up to 1.2 km	Radio Frequency Jamming	Disrupts communication between the drone and its operator. Can force the drone to land or return to its starting point.
7	Rafael Drone Dome	Up to 3.5 km	RF Detection and Jamming,EO/IR sensor	Provides 360-degree, rapid detection and neutralization of multiple drones simultaneously.
8	Elbit Systems ReDrone	Up to 10 km	RF Detection and Jamming, EO/IR sensor	Detects, identifies, tracks, and defeats hostile drones. Offers a variety of countermeasures
9	Zen Technologies	Up to 4 km	RF Based Drone detector (RFDD)Video based Drone Identification	Tracking (VDIT)Radar Data fusion and Command Center (DFCC)Drone RF Jammer (DRFJ).It has real time awareness of the situation.It has an integrated all current weapons suite and infrastructure.It also has a synergistic combination of 9-10 technologies and a 24X7 persistent and autonomous monitoring and tracking service

Detection Module: Utilizing ultrasonic sensors, specifically the HCSR04, as radar trackers forms the backbone of the system. These sensors emit high-frequency sound waves and detect echoes from objects in their path. By strategically placing these sensors, the system can effectively detect the presence of drones entering the restricted area. The sensors measure the time it takes for the sound waves to return, enabling accurate distance calculations and detection.

Image Processing Module: A crucial component of the system is the integration of a camera module, particularly the ESP32, for visual identification and tracking. Upon detecting a drone, the camera captures its image, which is then processed using sophisticated algorithms. These algorithms analyze the captured images to identify whether the detected object is a drone or another type of object. This information aids in precise tracking and targeting of the drone

Fig. 1. Detection Module

Fig. 2. Image Processing Module

Neutralisation Module: The system employs servo motors to control the direction of a laser beam, facilitating targeted destruction of the detected drones. Once the drone is identified and tracked using the detection and image processing modules, the system uses servo motors to adjust the position of the laser beam accurately onto the target. An Arduino Uno microcontroller coordinates the movements of the servo motors based on the drone's position, ensuring precise targeting. Upon successful targeting, the laser is activated to disable or destroy the drone, thus neutralizing the threat.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

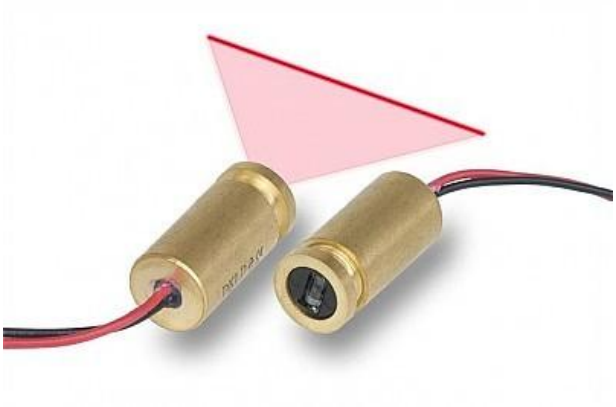

Fig. 3. Image Processing Module

Integration and Coordination: The various components of the system, including the ultrasonic sensors, camera module, servo motors, laser, and Arduino Uno microcontroller, are integrated and coordinated to work seamlessly together. The Arduino Uno acts as the central processing unit, receiving input from the sensors and camera, processing the data, and controlling the servo motors and laser accordingly. This integration ensures efficient and effective operation of the antidrone system.

Strategic Deployment: The system is strategically deployed in high-security or restricted zones where the presence of unauthorized drones poses a threat. By placing the detection sensors and camera modules at key entry points and sensitive areas, the system can effectively monitor and respond to drone incursions. Additionally, the flexibility of the system allows forscalability and customization based on the specific security requirements of the area.

Continuous Monitoring and Improvement: To ensure optimal performance, the anti-drone system undergoes continuous monitoring and improvement. This includes regular maintenance checks, calibration of sensors and cameras, and software updates to enhance functionality and address anypotential vulnerabilities. Additionally, ongoing research and development efforts are conducted to incorporate new technologies and methodologies for even greater effectiveness in countering drone threats.

Overall, the methodology for countering unauthorized drones in high-security zones is a comprehensive and multifaceted approach that combines detection, image processing, and Neutralisation capabilities. By integrating advanced technologies and strategic deployment strategies, the system provides a robust defense against the evolving threat posed by unauthorized drones.

Algorithms used in our Project:

We are Looking to use Iterative and Incremental model of Software engineering for our project development because of certain factors like flexibility, Iterative development, Continous testing, Risk mitigation etc. This model will be showed to client and changes can be made as per his requirements

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

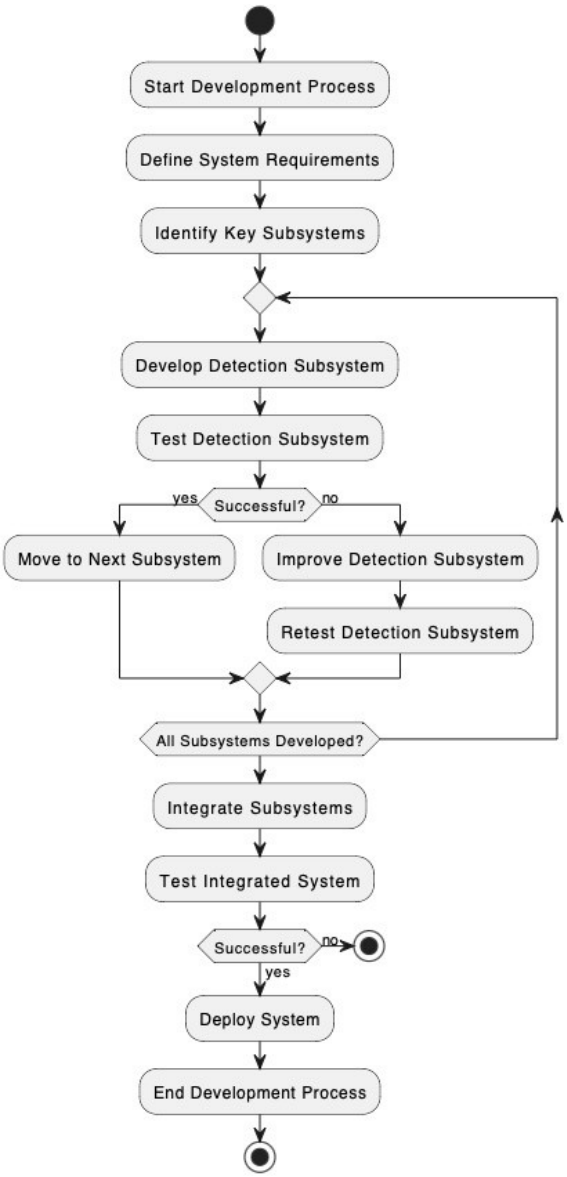

Fig. 4. Detection Module Algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

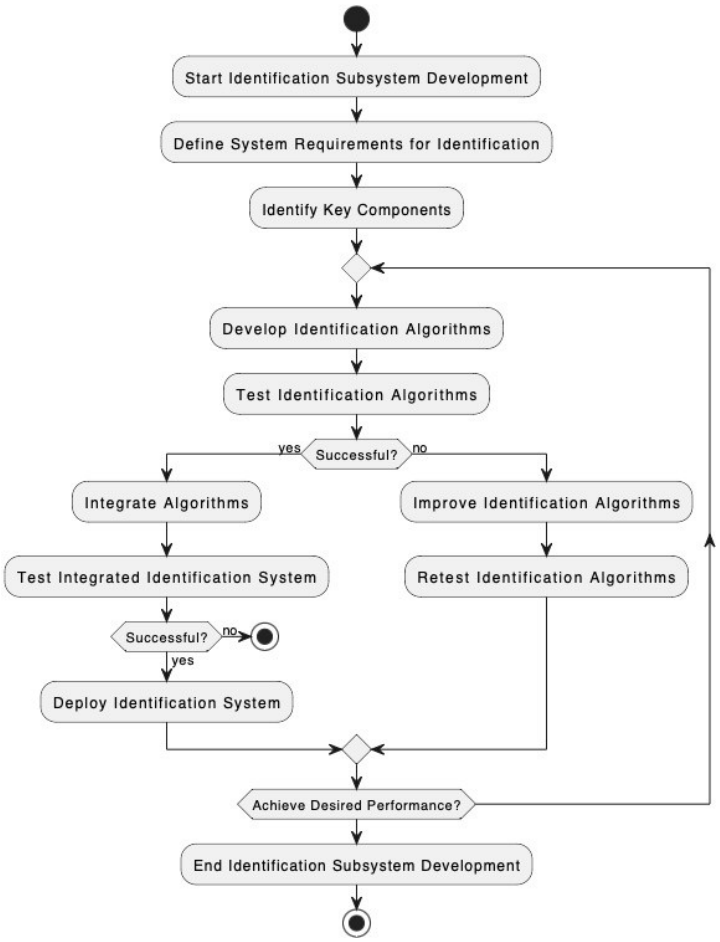

Fig. 5. Identification Module Algorithm

Mathematical Model:

Module 1: Detection Module

Let's denote: d as the distance from the ultrasonic sensor to the detected object. t as the time taken for the ultrasonic waves to travel to the object and back. v as the velocity of sound in air.

Then, we can use the formula:

$$d=1/2\ vt$$

Module 2: Identification Module

We can represent the identification process mathematicallyusing image processing algorithms. Let's denote: $I(x, y)$ asthe intensity of the image at pixel (x, y). $D(x, y)$ as the dronedetection binary image where $D(x, y) = 1$ if the pixel (x, y)corresponds to a drone, and $D(x, y) = 0$ otherwise. $B(x, y)$as the bird detection binary image where $B(x, y) = 1$ if thepixel (x, y) corresponds to a bird, and $B(x, y) = 0$ otherwise.We can use various image processing techniques such as edge detection, contour analysis, and classification algorithms to identify drones and birds in the captured images.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

Module 3: Neutralization Module

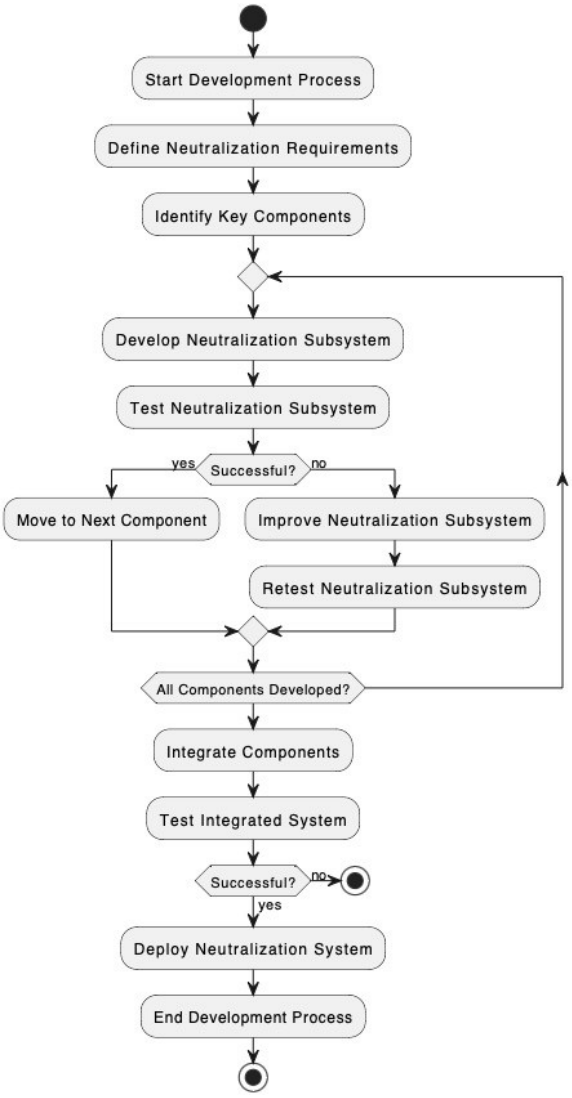

Fig. 6. Neutralisation Module Algorithm

For the neutralization module, let's denote: L as the laserpower. t_n as the time duration for which the laser is fired. We can represent the neutralization process as:

$$E_{\text{drone}} = L \cdot t_n$$

Where E_{drone} represents the energy delivered to the droneby the laser.

Procedure:

System Implementation PlanProject Objectives:

- Develop an integrated Anti-Drone System capable of detecting, tracking, and neutralizing threatening drones.
- Utilize image processing, radar, sensors, and laser technologyfor effective threat mitigation.
- Ensure the system is reliable, accurate, and safe for deployment in various environments
- Comply with legal and ethical guidelines for drone countermeasures.

Project Phases:

Phase 1: Project Initiation (Month 1): Define projectscope, objectives, and success criteria.

- Form the project team and allocate responsibilities.
- Develop a project timeline and budget.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

- Establish communication and reporting protocols.

Phase 2: Requirements and Research (Months 1-2)*:* Research current drone threats and countermeasure technologies.

- Define technical requirements for the Anti-Drone System.
- Identify legal and ethical considerations.
- Develop a risk assessment and mitigation plan.

Phase 3: System Design (Months 2-3)*:* Develop system architecture, including hardware and software components.

- Design the laser-based neutralization system.
- Create user interfaces for operators and administrators.

Phase 4: Prototyping (Months 3-4)*:* Build a prototype of the Anti-Drone System Radar Module.

- Testing detection of our project prototype.
- Refine the system design based on prototype feedback.

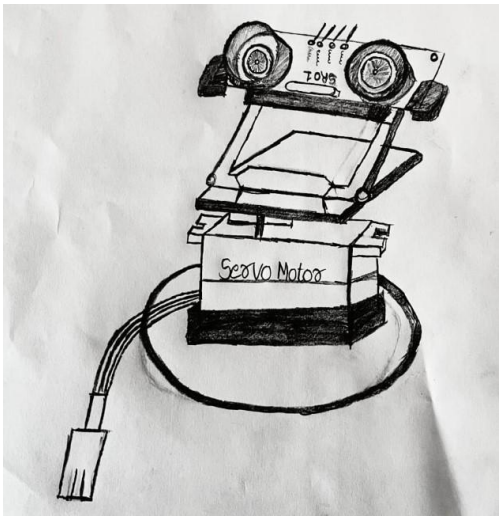

Fig. 7. Radar Module.

Phase 5: Prototyping phase 2 (Months 4-5)*:* Build aprototype of the Anti-Drone System Laser Module.

- Testing for intruder drone and neutralise it.
- Evaluate system performance and accuracy.
- Address any identified issues and refine the system.

Phase 6: Prototyping phase 3(Months 5-6)*:* Developand optimize image processing algorithms.

- Integrate and calibrate radar and sensor systems.
- Conduct comprehensive testing and quality assurance.

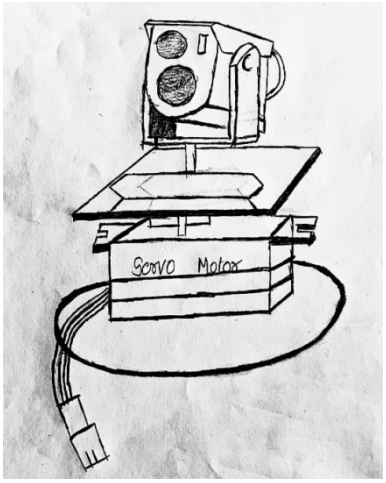

Fig. 8. Laser Module.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

Phase 7: Deployment and Testing (Month 6-7): Prepare for the deployment of the Anti-Drone System in target environments.

- Train operators and maintenance personnel.
- Develop documentation and training materials.

V. RESULTS AND DISCUSSIONS

Observations

Test Cases: The test cases were divided into two primary categories: Blackbox testing and white box testing. Blackbox testing entailed scrutinizing the system's hardware overview, while white box testing concentrated on evaluating the functionality of the code, encompassing inputs, outputs, and overalloperation. Test cases for this project were classified under blackbox testing, which encompassed the examination of both the system's overview component and its operational functionality. This approach ensured a comprehensive assessment of the system's behavior, encompassing both its structuralattributes and its operational effectiveness. By delineating these test cases into distinct categories, the evaluation process facilitated a thorough examination of the system from various perspectives, ultimately contributing to the identification and resolution of potential issues or discrepancies.

Overview (Blackbox testing): Rigidity and Impacton system.

Component testing (Blackbox testing): Testing ofsensors, motors and microprocessors.

Work Testing (Whitebox Testing):System performance range and accuracy in detection and identification.

Sr.No	Test Case	Predicted	Actual	Result
1	Is Ultrasonic&Servo working?	Yes	Yes	Detection Active
2	If Obj less than 60cm ?	No	No	PCB Pin low for camera
3	If Obj in between 0-60cm?	Yes	Yes	PCB Pin high for camera
4	Is ESP 32 Module onx?	Yes	Yes	Identification Active
5	If ESP 32 identified as Drone?	Yes	Yes	PCB for Laser and radar high
6	If ESP32 identified as Drone?	No	No	PCB laser low and radar high
7	Is Laser Working ?	Yes	Yes	Neutralization Active
8	If Laser fired?	Yes	Yes	Neutralization done
9	If Laser not fired?	No	No	No Neutralization
10	If Drone Neutralised	Yes	Yes	System working
11	If Bird Neutralised	No	No	System working

Working Modules

We are Looking to use Iterative and Incremental model of Software engineering for our project development because of certain factors like flexibility, Iterative development, Continoustesting, Risk mitigation etc. This model will be showed to clientand changes can be made as per his requirements.

Project was divided into 3 main modules which includes

Detection Module -The primary goal was to develop a detection radar capable of identifying aerial objects from a distance equivalent to 60 centimeters (with each 10 centimetersrepresenting 1 kilometer). To fulfill this requirement, we optedto utilize an ultrasonic sensor HC-SR04 in conjunction with a servo motor for sensor rotation.

Identification Module -The main aim of this module is to distinguish between birds and potential threats, such as small drones. Due to similar image signatures of small drones and birds on radar screen, accuracy and the protection of living organisms were paramount. Hence, we chose to develop this system using the ESP32 CAM MODULE, equipped with a 2MP camera sensor, sufficient for identification within a 60cmrange.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

Neutralization Module -Utilizing a hardkill method to eliminate drones required pinpoint accuracy. A laser-based neutralization technique proved most suitable for its abilityto neutralize both pre-programmed and controlled drones effectively.

Module 1: Detection Module This module is responsible for detecting small threat causing intruder drones in restricted areas Especially no fly zones. it uses ultrasonic sensor which responsible to detect and perform 24 * 7 surveillance in particular zone

- **Input:** A transmitter present in HC-SR04 emitssound waves, while a receiver present in same sensor detects and sends signal to GUI based processing if these waves bounce off an object, serving as radar input to alertthe system of an intruding drone.
- **Output:** A graphical user interface (GUI) for radaris being developed to show the distance and direction of an object on the screen. It also activates a camera modulesimultaneously for prompt identification.

Working:

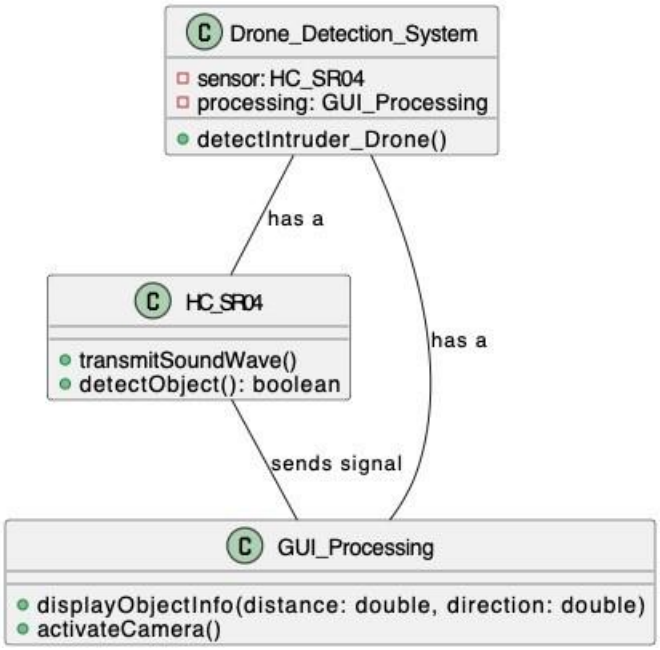

Fig. 9. Working of Detection Module.

Module 2: Identification Module This module is responsible for Identifying between Drone and bird .It uses ESP32 Cam Module who responsible to identify accurately and providing safety to living organisms like birds and also helping systemto take accurate decision.

- **Input:** Once triggering signal is recieved Camera module comes into action and help system to take decisions about neutralising object or not by performing image processing.
- **Output:** There will be 2 possible output for this if system identifies it as an intruder drone it will trigger laser module and if Not identified as intruder drone or identified as bird or other living organism system will cancel out next step but radar will still in surveillance mode.

Module 3: Neutralisation Module This module is designed to eliminate threatening drones using the Hardkill method. We utilize a laser module for precise and accurate targeting, ensuring cost efficiency while effectively neutralizing drone threats.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

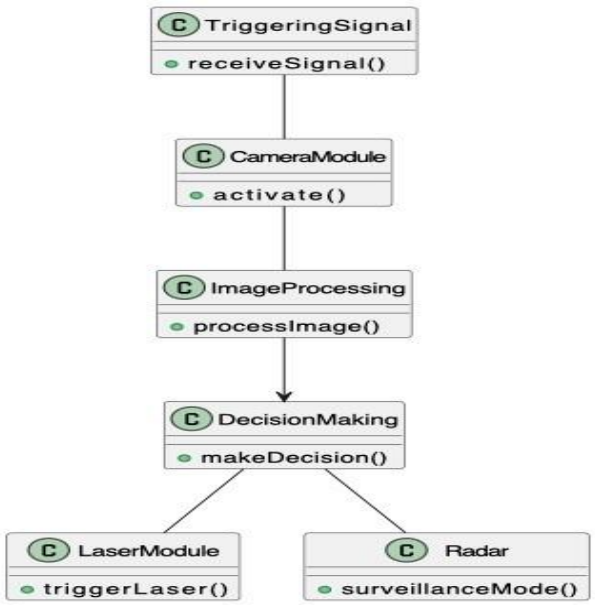

Fig. 10. Identification Module Working.

- **Input:** As soon as processing of identification module is done and incomming object is identified as threat casusing drone adaptive measures will be takenand laser will be fired to cause malfunctioning in drone.
- **Output:** Once drone is neutralised laser pin will be set to 0 and detection will be continued to find another target.

Working:

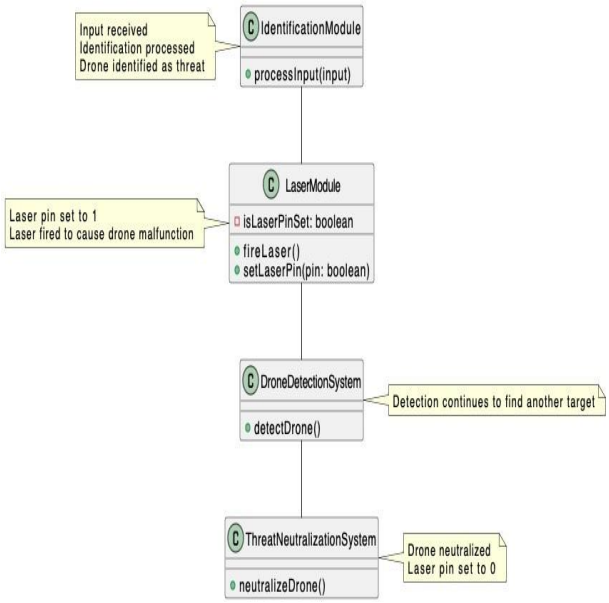

Fig. 11. Neutralisation Module Working

VI. CONCLUSION

Finally, our anti-drone system provides a comprehensive response to the mounting threats posed by drones. It enables enterprises and individuals to protect their interests in a developing aviation scenario by assuring increased security, safety, privacy, regulatory compliance, and critical infrastructure protection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

The ”Anti-Drone System” project introduces a versatile and innovative technology applicable in various sectors. It serves to protect critical infrastructure, like power plants, airports, and government buildings, by detecting and neutralizing unauthorized drones. It also ensures security at major events such as sports competitions, concerts, and political rallies, where rogue drones could pose threats. Prisons benefit from preventing drone deliveries of contraband. Law enforcement uses it for crowd control, public event monitoring, and search and rescue operations. Border security agencies employ the system to detect and counter drones attempting to cross national borders, addressing smuggling and intrusion risks. In military and defense, it safeguards against espionage, reconnaissance, and drone-based attacks. The corporate world uses it to protect data centers against industrial espionage. During natural disasters, it secures airspace for first responders. It upholds individual privacy by preventing drones from capturing unauthorized imagery. Research institutions and labs protect intellectual property. In agriculture, it safeguards fields from pests and drone-based attacks. Sports and entertainment venues enhance spectator safety and prevent disruptions during events. Highprofile individuals use it for VIP protection. The ”Advanced Anti-Drone System” project adapts effectively to address a wide range of security concerns across various sectors, ensuring the safety, privacy, and functionality of critical areas and events.

VII. ACKNOWLEDGMENT

First and foremost, we express our deep sense of gratitude, sincere thanks and deep sense of appreciation to Project Guide Prof. D. S. Rajnor, Department of Computer Engineering, SNJB’s Late Sau. K. B. Jain College of Engineering Chandwad, your availability at any time throughout the semester, valuable guidance, opinion, view, comments, critics, encouragement, and support tremendously boosted this project work. Lots of thanks to Head, Computer Engineering Dept., Dr. Kainjan M. Sanghavi for providing us the best support we ever had. Your opinion, view, comments and thoughts have really helped me to improve my writing. We like to express our sincere gratitude to Dr.R.G.Tated, Principal, SNJB’s Late Sau. K. B. Jain College of Engineering, Chandwad, for providing a great platform to complete the thesis within the scheduled time. We are also Thankful to all the faculty members, Computer Engineering Department, SNJB’s K. B. Jain College of Engineering, Chandwad, for giving comments for improvement of work, encouragement and help during completion of the stage 1 project work. Last but not the least; we should say thanks from the bottom of our hearts to my Family Friends for their never-ending love, help, and support in so many ways through all this time. Thank you so much, and finally, we are thankful to MIGHTY GOD, who gives us the courage, confidence not only for this Dissertation work but also in bad difficult situations..

REFERENCES

[1] Tung-Ming Koo and Hung-Chang Chang and Guo-Quan Wei,Construction P2P firewall HTTP-Botnet defense mechanism,IEEE International Conference on Computer Science and Automation Engineering,2011,1,33-39,Aug,
[2] Hyunsang Choi and Hanwoo Lee and Heejo Lee and Hyogon,Botnet Detection by Monitoring Group Activities in DNS Traffic,booktitle=7th IEEE International Conference on Computer and Information Technology,2007,715-720,oct,
[3] Choi, Hyunsang and Lee, Heejo and Kim, Hyogon,BotGAD: detecting botnets by capturing group activities in network traffic,Proceedings of the Fourth International ICST Conference on Communication System Software and Midleware,2009,1-8,oct,
[4] Govil and G.Jivika,Criminology of BotNets and their detection and defense methods,IEEE International Conference on Electro-Information Technology,2007,215-220,sept,
[5] Craig A and Jim Binkley and David Harley,Botnets: THE KILLER WEB APP,SYNGRESS,2007,