ANONYMOUS DETECTIONS IN FLIGHT LANDING

A. Vinitha[1], T. Ayyapparaj[2], P. S. Sumathi[3]

ABSTRACT

In aviation, safety has always been a top priority and this has been shaped over time by various innovations that keep revolutionizing the management of aircraft at crucial times such as when landing. One of these, so-called anonymous detection systems i.e. technological systems that monitor, track and detect aerial threats or unregistered aircraft without reveal the user identity, has elicited considerable interest. This writing paper will discuss the significance of anonymous detections at an airport during landing, the technology involved in these systems, the cyber security parts and the issues of using such a solution in contemporary aviation infrastructure.

Keywords : Anonymous Detection Systems, Aviation Safety, Passive Radar Technology, Sensor Fusion, Cybersecurity in Aviation, Unidentified Aerial Vehicles (UAVs)

I. INTRODUCTION

During the last several years, there has been a lot of attention paid to the aviation systems because of the rising air traffic, the weaknesses in cybersecurity, and the risks caused by drones. landing is known as one of the most vulnerable stages of a flight that needs precision, coordination, and knowing whether it is able to land or not. the existing air traffic control (atc) structures based on radar, transponders, and communication use these tools to guarantee safety, and its mechanisms may not be always sufficient at confronting the unknown or anonymous air entities. Detecting aircrafts or drones without revealing their identity indicates the

Department of Computer Science[1]
Karpagam Academy of Higher Education
Coimbatore, Tamilnadu, India[1]
vinitha.archimedies@kahedu.edu.in[1]

Department of Computer Science[2]
Sree Narayana Guru College, Coimbatore, Tamilnadu, India[2]
ayyappan.sngc@gmail.com[2]

Department of Computer Science[3]
Government Arts and Science College, Chennai, Tamilnadu, India[3]
sumisundar.ps@gmail.com[3]

* Corresponding Author

anonymous detection of this aircraft or drone, which may be intentionally malicious or systemic. These systems need to be able to work without depending on the cooperation of data of the aircraft via passive and active sensing strategies. this paper goes to great depth to examine the functioning principles behind those systems, their value to flight landing, and the future of air traffic management.

II. VULNERABILITY UPON LANDING

The most danger prone moment of the aircraft is during take-off and landing and in aviation accident, it is observed that about 49 percent of air accidents take place during take-off and landing. In the landing process, the pilots rely on the navigation systems, air traffic control cooperation, and the help of the ground. An unidentified target or unauthorized plane in controlled airspace can grossly affect safety which may result to excruciating diversions, and emergency measures.

A. Successful Blame diagnosis The Game

Known surveillance is based on information by communication and navigation systems including on-board and radars [1]. The present systems find it hard to pick threats that deliberately do not want to be identified This includes: Rogue Aircraft: An aircraft, which is not transmitting any identification signal or transmitting misleading information (intentionally). Unmanned Aerial Vehicles: Drones that do not have transponders or are out of controlled airspace. Airspace security gets additional challenges with the rise in UAVs usage [2]. Stealth Aircraft: This is an aircraft that is designed to reduce chances of radar detection and it might even find its way into airspace without even a prior permission [3].

1) The Systems that are present are Weak

There is one weakness with the existing systems when it comes to control of these threats: Transponder dependency: The legacy ATC systems are transponder dependent to identify and denote the plane. Disabled or not operational transponders in planes eliminate air traffic control systems. Radar Vulnerabilities: As much as radar is a major surveillance asset, it may be bounded by the topography, weather, and the design of stealth aircraft [4]. Also, sets of radar are jamming and spoofing [5].

Cybersecurity: The aviation sphere has been more concerned with the problem of cybersecurity [6]. The aircraft are even getting connected further exposing them to cyberattacks [7].

B. Solutions that can be taken Developing Anonymity
1) Advanced Radar Technologies

Multistate Radar : To enhance the detection ability to include highly stealthy airplanes; this is by employing multiple radar receivers together with transmitters. VHF Radar: Using VHF radar that happens to shed some light on stealth aircraft as compared to the conventional microwave radar [8]. Passive Radar: Radar systems which spots aircraft by examining the reflection of other radio or TV signals back towards them, from any other source.

2) Sensor Fusion

Creating Combinations: Combining data of various sensors, which can be radar, acoustic sensors, or optical cameras, to create a complete image of the airspace [8].
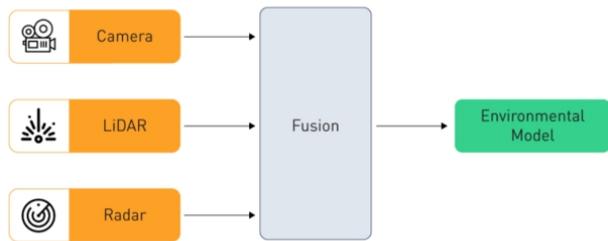

Fig 1 : Sensor fusion of Camera, LiDAR, and Radar to build a unified environmental model.

Machine Learning: Employing machine learning models to read the data provided by the sensors and determine abnormal detected patterns which could be a sign of threat [9].

3) Enhanced Cybersecurity Measures

Intrusion Detection Systems: Installation of systems to detect and reply to attack on aircraft and ATC infrastructure by cyberattacks [10]. Secure Communication Protocols: Secure communication channel using endo to end encryption to ensure data is not intercepted and help to avoid spoofing.

C. The Importance of Emergency Landing Systems

The necessity of having strong emergency landing solutions is closely linked to the possibility to monitor the appearance of unrecognized aircraft: UAV Emergency Landing: The creation of systems that are capable of detecting safe terrains that UAVs may land in emergencies or when other unauthorized aircraft are near [11][12]. Autonomous Landing: Introducing autonomous landing systems whereby aircraft can safely land devoid of the use of bad ground-based systems that can be compromised.

D. Rise of Unmanned Aerial Vehicles
1) Proliferation of UAVs in Civilian Airspace

The number of drones and other UAVs that are encountered in the civil airspace has been on the rise (Telli et al., 2023). It is expected that logistics and transport drone market in the entire world will increase up to approximately 29.06 billion dollars by 2027 [13]. Such a growth has its opportunities, and challenges: Airspace Congestion: As it is already, the congestion of airspace is increasing as a result of the spreading of other UAVs, particularly in the vicinity of the airport. Safety: Most of the UAVs are not legitimately registered or have the transmission of identifying signals. These are capable of disrupting commercial flights particularly when they are making a landing at a crowded airport. Security Threat: UAVs may inflict unlawful purposes, including regular observation or smuggling, that is, a safety hazard to vital facilities and the safety of the population [14].

2) The Need for Anonymous Detection Systems

Anonymous detecting systems are necessary to sort out the legitimate aircraft and the unidentified or unregistered aircraft. These systems must be allowed to follow the following: Identification of the UAVs that do not broadcast messages giving out identification. Classification of UAVs: This involves the division of the various types of UAVs into one in relation to the flight path and data of the information obtained by the sensor [15]. Real time tracking of UAV: The ability to track the mobility of UAVs to make sure that they are in regulated airspace.

3) Challenges in UAV Detection

The issues of UAVs detection are associated with a number of issues: Unstoppable: Mini Unmanned Aircraft Vehicles (UAVs) are too small as well and they cannot be brought down using ancient radar sensors [9]. Low Altitude Operation: UAVs normally perform in the low altitude environments and hence cannot be easily detected in a clutter on the ground. Variety of Flight Characteristics: There are varying flight characteristics of UAVs and this may create difficulties in coming up with detection algorithms that will work on all relevant types of UAVs.

Limited visibility night: A detection of the UAVs at limited visibility or during the night is the biggest threat to security [7]. UAVs can be detected by using thermal infrared cameras in daytime and at the night because they detect slight differences in heat [7].

E. Proposed Solutions: Enhancing Anonymity Detection

1) Advanced Radar Technologies

Multistate Radar: This involves setting up multiple radar receiver and transmitters to be used in improving its barriers detection and in particular that of stealth aircraft. VHF Radar: By using the new radar through VHF radar that is more capable of locating the stealth aircrafts than microwave radar. Passive Radar: Radar which detects other object by observing (in some other emission) a radio emission or a TV emission reflection off a barrier.
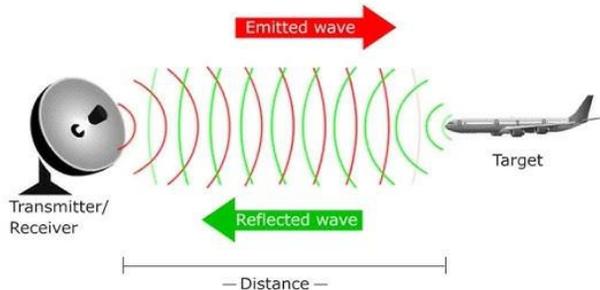

Fig 2 : Radar detects target via emitted and reflected waves.

2) Sensor Fusion

Combining Data: Integrating data from multiple sensors, such as radar, acoustic sensors, and optical cameras, to create a more comprehensive picture of the airspace. Machine Learning: Using machine learning algorithms to analyze sensor data and identify anomalous patterns that may indicate a threat.

3) Enhanced Cybersecurity Measures

Intrusion Detection Systems: Installing notification that detects and machineries respond to hacking of plane and ATC infrastructure. Secure Communication Protocols: The practice of using encrypted communication channels to make sure spoofing and interception of information cannot take place.

4) The Importance of Emergency Landing Systems

The ability to detect unidentified aircraft is closely related to the need for robust emergency landing systems: UAV Emergency Landing: Developing systems that can identify safe landing zones for UAVs in case of emergencies or when unauthorized aircraft are detected [13]. Autonomous Landing: Implementing autonomous landing capabilities that allow aircraft to safely land without relying on potentially compromised ground-based systems [13].

III. TECHNOLOGY BEHIND ANONYMOUS DETECTION SYSTEMS

Anonymous detection technologies combine elements of radar, radio frequency analysis, artificial intelligence, and computer vision to monitor airspace. These systems are designed to detect and track aircraft that may not be broadcasting their identity or are intentionally trying to avoid detection. The use of radar, radio analysis, artificial intelligence and computer vision paired together to the monitoring of the airspace are ways of detecting the presence of the anonymous technologies. The systems are used to identify and trace advanced aircraft, which might not be putting its information in the air, or trying to avoid getting its information.

A. Radio Frequency Sensing and Portable Radar

Unlike the classical radars, which emit the signal and wait until it is reflected, passive radars also use the already present radio waves (TV towers, GPS, etc.) to detect aircraft [17]. This qualifies them to be used in the non-intrusive and covert tracking. The passive radar is a newer technology that takes advantage of the make-up of non-cooperative targets, in that, they do tend to reflect on ambient available radio waves [21]. The RF sensors can read the signals which are sent out by on board equipment like GPS despite having aircraft transponders switched off.
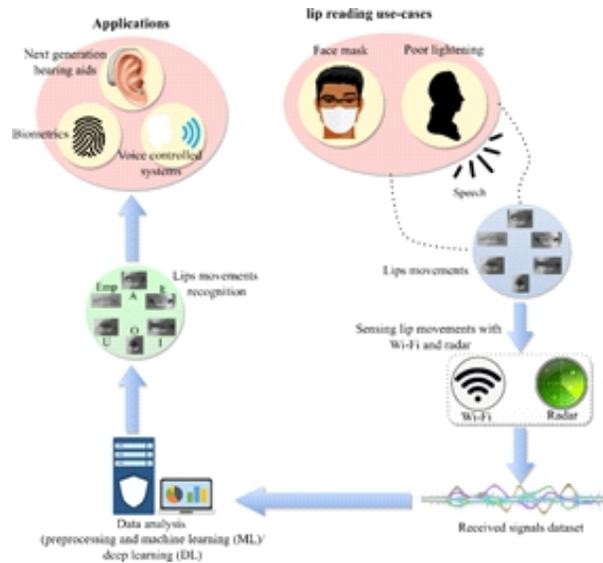

Fig. 3 : Lip reading using Wi-Fi/radar for smart audio and biometric applications.

1) Advantages of Passive Radar

Surreptitious Activity: The active radars do not transmit their own signals hence they are hard to locate. Wide Area Coverage: Since radio wave sources do not need to be

dedicated transmitters, the sources of radio waves (both natural and man-made) can be used to provide wide area coverage. Cost-Effective: The passive radar could also be cheaper than the conventional radar systems since no deployment of dedicated transmitters and their maintenance would be required.

2) Challenges of Passive Radar

Signal Dependency: Passive radar system needs an external source of radio waves and this may just not be there in some places. Signal Clutter: The passive radar works are liable to scrutiny by other kinds of signal clutter, as in radio and television broadcasts. Limiting Detection Range: Passive radar systems can have a limiting detection range which is defined in terms of strength of the radio waves used as the outside signal and the frequency of those same radio waves.

B. Multistatic Radar Networks

With multistate radar systems, an abundance of transmitters and receivers are used. This is able to be triangulated and objects located according to their interactivity with the signal environment. These systems can be very effective in identifying the stealth planes, or with the low radar signature drones.
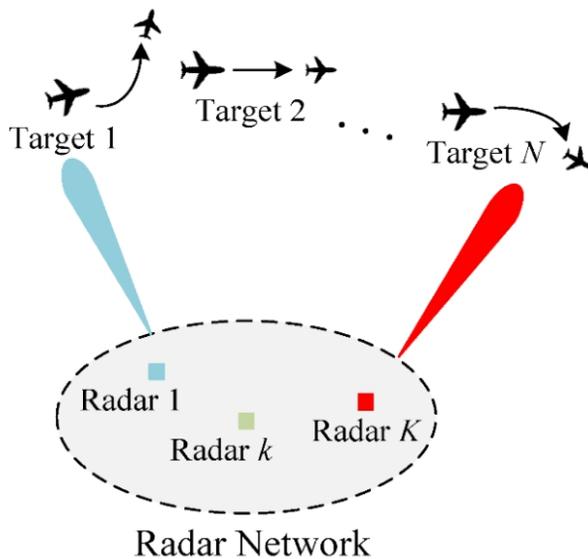

Fig 4 : multi-radar network tracking multiple aerial targets.

1) Advantages of Multistatic Radar

Enhanced Detection: The multistate radar has the possibility of regaining a better detection than conventional radar, especially in the stealth-section and drones. • Improved Tracking Reliability: Tracking accuracy of a multistate radar provides greater capability of tracking the aircraft due to the ability to triangulate on the location of the aircraft. • Enhanced

Coverage Area: Multistate radar allows coverage area to be enhanced relative to coverage area with the traditional radar systems, since the receivers can be distributed over a greater area.

2) Challenges of Multistatic Radar

Complex System Design: The multistate radar system designs are more complex as compared to the conventional radar system and so need a complex system that is complex to deploy. Data Fusion Requirements: Multistate radar systems have their data fusion algorithm needs that are extremely difficult. Synchronization Problems: The multistate radar systems also have to ensure precision on the synchronization of the transmission and the reception, so that flawless tracking can be established.

C. Electro-Optical and Infrared (EO/IR) Systems

The sensors are the EO/IR that are able to identify objects by heat signature or the visible light. These systems allow visual detection of objects in case of the low-visibility caused by fog or rain and complement radar. UAVs can even be detected at night by looking at them with thermal imaging because they detect any slight changes in heat (Andra# jaw e advantage pilot sold system l t e grand quote

1) Advantages of EO/IR Systems

Visual Identification: The EO/IR systems can visually identify aircraft and thus operators get to identify the aircraft type of airplanes. Low-Visibility Detection: The EO/IR systems have the ability of detecting the low-visibility aircraft either when it is raining or/and within the fog. Passive Detection: EO/ IR systems are calling passive meaning they are hard to pick because they are sensitive and that makes them difficult to detect.

2) Challenges of EO/IR Systems

Weather : The short distance of detection by EO/IR systems is also a limitation which can be occasioned by weather conditions as well as the size of the aircraft. False Alerts: False alerts can be made on EO/IR systems as they can be less specific to other heat sources released by an intruder e.g. fires or sunlight. Image Processing Needs: The EO/IR systems must apply advanced image processing algorithms to have a detection and tracking situation of the airplane.

D. AI and Pattern Recognition

Through the radar and sensor-gathered data, machine learning algorithm is used to distinguish between manned aircraft, drones, and birds [5]. It is also possible to forecast flights routes and identify irregularities in flights with AI, e.g.

presence of a flying object, not broadcasting its details in a restricted air area. Anomaly detection works well on hard to predict unexpected events but Anomaly scans have too many false positives and are sometimes dependent on tuning related to the domain [5].

1) Advantages of AI and Pattern Recognition

Enhanced Detection Precision: AI and Pattern recognition algorithms also aid in enhancing the detecting accuracy of the airplane because it will be taught how to differentiate between various planes and other items. Anomaly Detection: It is also possible to apply AI when detecting anomalies with the behaviors of aircraft, e.g. an unauthorized flight or flights of plan. Automated Threat Assessment: AI may be able to automate the process of assessing the threat and operators can be able to detect the threat and act swiftly.

2) Challenges of AI and Pattern Recognition

Data Requirements: AI and other algorithms of pattern recognition needs massive data to train at a good level. Computational Resources - AI and the pattern recognition algorithms can be very computational and they may require very powerful system hardware. Explainability: AI algorithms are complex to interpret, and therefore, it is hard to fathom why a given decision was recommended by AI algorithms.

IV. CYBERSECURITY ASPECTS

A. Anonymity vs. Security

Anonymity is a two-sided coin. On the one hand, it guarantees privacy of users in civil uses; on the other hand, it allows bad players to abuse the airspace. Aviation cybersecurity should thus not be completely closed but should be opened up sufficiently. One should bear in mind that the loss of privacy can be an element of the digital device dependency (exploring Digital Dependency And Psychosocial Functioning: A Study On Well-being Of Adolescents, n.d.). The capability of hostile parties to target airspace may take cyberspace cyberattacks, which can result in such massive consequences like monetary costs and image consequences [11].

B. Spoofing and Jamming Detection

Anonymous detecting systems are frequently implemented in conjunction with anti-spoofing systems that detect fake signals of the GPS [19] or jamming systems. These are vital during landings on satellites-based navigation. Spoofing can make the airplane go to the incorrect destinations [21]. Jamming attacks have the ability to cut off

data transfer between bona fide users [20]. Such threats can only be impeded through the aid of robust models of data declarations and codes [15]. Physical layer spoofing can be used to intervene with wireless communication and alter the conveyed information on the malicious links [13].
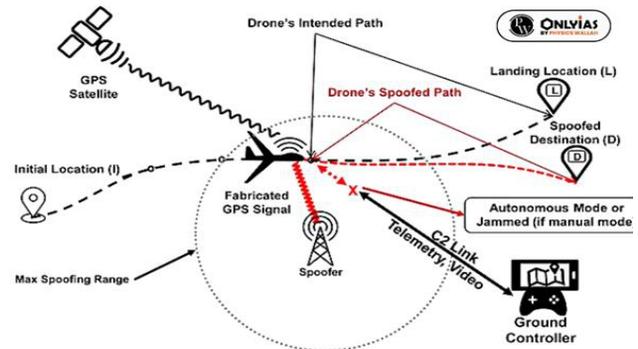

Fig. 5 GPS spoofing diverts drone from intended to fake destination path.

C. Encrypted Communication Monitoring

Anonymous detection systems retrieve signal metadata, consisting of their strength, frequency, and timing, without decryption, even by evading the privacy laws, such as the strength level of the signal, frequency, and timing; all of which are monitored and can reveal the existence of an aircraft [13]. The radio network promotes safe passage of field data to the central system, and the security is encrypted [5].

V. APPLICATION IN REAL-WORLD SCENARIOS

A. Airport Security

Major airports across the globe that include Heathrow, JFK, and Changi are in the process of testing, or have implemented radar, RF and EO/IR-based drone detection systems. Such systems warn the controllers of the presence of any unauthorized aerial vehicles that may cause interference to landing flights. The use of such systems is necessitated by the rising popularity of drones and the security and safety issues that they can cause [16].

B. Military and Civilian Cooperation

Civilian versions of military-grade, surveillance-based tools are being implemented previously restricted to armed forces. One of them is an extension of passive radar to joint civil-military airspace surveillance within the NATO. Furthermore, presence in a very real-life scenario of military operatives and counter-UAV technology has provided credence and technical prowess to assist civilian airports Chess Dynamics Counter-UAV Technology Features on Panorama.

C. Drone Incidents and Emergency Diversions

According to Gatwick Airport Drone Incident, in 2018, the airport was seriously disrupted by sightings of the drones. This went over 140,000 people who were passengers. Had the anonymous detection systems been present, it is possible that the UAVs would have been detected early enough, and the situation would have been tackled faster. But in the wake of the incident, speculations arose as to it having been either a bird, or a plastic bag, a balloon, a paper lantern or even a far manned aircraft that must have been the so-called drone.
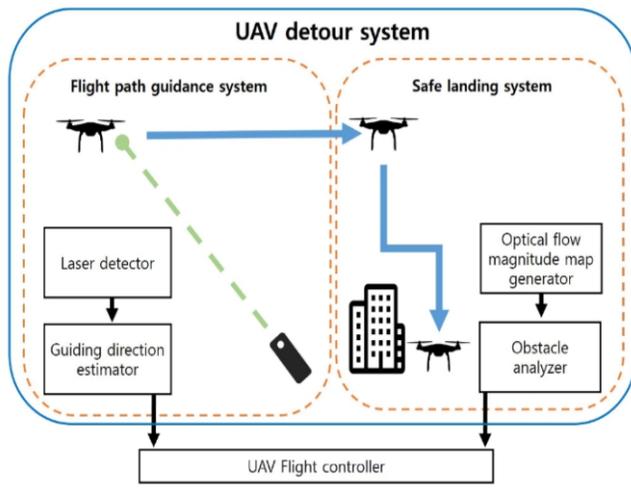

Fig. 6 : UAV detour system that guides the flight path and safe landing though analysis of the obstacles.

VI. CHALLENGES IN IMPLEMENTING ANONYMOUS DETECTION

A. Technical Limitations

Some limitations that are associated with the detection systems are as follows: False Positives: It is known to enter into false alarms associated with birds or even weather conditions or even plastic bags. Low Altitude Coverage: Certain radars do not do a good job in identifying entities that fly at low altitude near the earth. Latency: Real time detection is also another important application especial when it comes to landing phases; any form of processing delays may make data go to waste. To illustrate, it can be noted that machine learning can be used to identify uncalibrated sensors in real-time.

B. Cost and Infrastructure

Anonymous systems of detection necessitate elaborate hardware installations, data processing centers, and those trained to use them. This is not possible in smaller airports. It is established by the FAA and the industry that the drone threat to airport security is a highly complicated issue.

C. Legal and Privacy Concerns

Surveillance of anonymous entities can be ethically controversial, on the one hand, it can imply obscure targeting of personal drones or air vehicles without justifiable reasons. There must be clearly spelt out legal provisions of what can and cannot be used to understand acceptable levels of monitoring. They ought to put into consideration privacy-enhancing technologies. There are privacy and surveillance issues that come out as AI is becoming more used in infrastructure digital monitoring [20].

VII. FUTURE OF ANONYMOUS DETECTION IN FLIGHT OPERATIONS

A. Integration with NextGen ATC

Next Generation Air Transportation is focused on modernizing the air traffic control with satellite navigations and digital communication. Blind detection systems also are in the scope of investigation that is supplementary to the airspace awareness. The major role of ATC is to secure safe distances among planes, facilitate ideal flight routes, and efficient communication between flight crews and air traffic controllers. The integration of AI into the ATC systems is associated with a variety of advantages that comprise added safety, better productivity, and more automation.
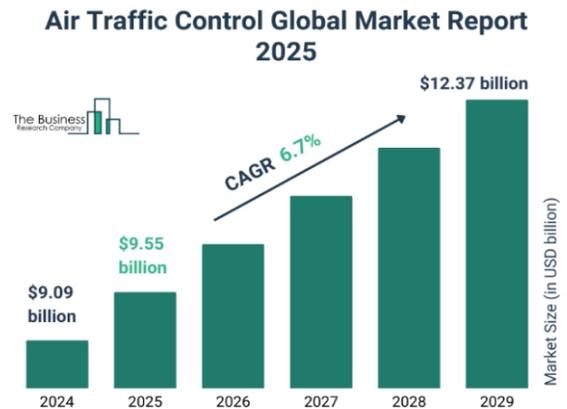

Fig 7 : Air traffic control market projected to grow at 6.7% CAGR, reaching $12.37B by 2029.

B. Role in Urban Air Mobility

When the air taxi and delivery drones appear in larger numbers in urban cities, anonymous detection will be essential to ensure that mid-air collisions do not occur, and to safeguard low-altitude corridors. UAM is a new kind of concept of air transportation based on the needs of passengers and loads in the city using drone capabilities. The demands should reflect the demands and disparities amidst city and country conditions.

C. Autonomous Landing Systems

Unmanned cargo planes are only some of the future aircraft that will have to land autonomously. Anonymous detection will serve as a backup, where nothing unfamiliar will be in the way of landing routes. The third involves some systems that recognize a secure landing area with reference to external databases or on-board sensors and thus access them within a potentially altered control model. An automated emergency landing system is the necessity to minimize the danger to the infrastructure, people, and aircraft.

VIII. CASE STUDY: DETECTING AN UNKNOWN UAV DURING LANDING

A. Scenario

A Boeing 737 is flying towards the big airport at the end of the day. There has occurred the unexpected presence of uncooperative UAV on the glide path. The UAV does not have any identification it broadcasts UAV detection may even be challenging at nighttime, in poor visibility conditions, and in the urban area. Such LSS targets have become an air threat both militarily and in civil senses.

B. Response by Detection System

The advantage of Passive Radar can be defined as the utilization of broadcast signals to detect the position of the object. By the speed and the way it moves, the AI classifier concludes that it is not a bird but a drone. They could use the machine learning algorithms and optimize the reliability and precision of the aircraft detectors. With the assistance of an infrared camera, it is possible to observe a heat pattern that most probably belongs to a battery-powered UAV. The system warns ATC, and the aircraft is made to land-off till the threat disappears.

C. Outcome

The possibility of a disaster is averted. It is then intercepted by counter-drone technology so as to land the UAV. Landing phases are critical, and any information must be detected in real-time, since no delay in processing the information will make it useless. Require privacy-preserving detection at subjected airports: Another preventative approach would be to install privacy-preserving detection systems at major airports as they will have a greater range and more traffic as the drone traffic increases and poses potential risks. Facilitate the cooperation between cyber and aviation professionals: This can involve both airports and aviation engineers, that together can increase the level of protection in the airports. Cooperation between any forms of security and aircraft engineers can guide security gaps and come up with strong security solutions. Introduce the AI-based systems to mitigate false alarms: AI-based and machine learning can be utilized in order to understand what is considered a drone and what is not, which can assist mitigation of false alarms and increase the accuracy of systems that detect them. Carry out frequent drills on the responsiveness of the systems: This can be used to gauge the responsiveness of the systems and enhance faster response in case of emergency. Such training is to run under a variety of circumstances, i.e., to engage drones of different types and weather patterns. Aviation legislation should be rendered up-to-date to include anonymous surveillance: Aviation acts should be put up to date to include anonymous surveillance since it is the only way through which clear laws can be established to clarify the levels of possible monitoring, as well as covering privacy rights. The presence of these legislations is projected to address the hoarding, retention, and exploitation of information that is retrieved by the use of anonymous recognition systems. You will have to achieve the right balance between privacy and security.

IX. CONCLUSION

Anonymity in flight landing is not only a technological breakthrough, but also an essential delivery mechanism in the field of aviation ready in future. With the progression of threats and higher volumes of air traffic, ensuring the safety of landing by responding and identifying the presence of a risk is a crucial issue of concern. Nevertheless, in spite of the unresolved issues, mainly in the matter of privacy verse odds versus surveillance, radar, artificial intelligence, and passive sensing, there is a flowering future ahead of them. Indeed, when these systems are integrated with the existing ATC systems, aviation infrastructure would be much more resilient and guarantee safer skies to everyone.

REFERENCES

[1] Lykou, G., Moustakas, D., & Gritzalis, D.. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. Informatica, 47..

[2] Telli, K., Kraa, O., Himeur, Y., & Amira, A.. A Comprehensive Review of Recent Research Trends on Unmanned Aerial Vehicles. Artificial Intelligence Review, 55, 6643-6703..

[3] Khawaja, W., Ezuma, M., Semkin, V., & Komarov, I.. A Survey on Detection, Classification, and Tracking of Aerial Threats using Radar and Communications Systems. IEEE Access, 10, 73131-73163..

[4] Alam, M. S., & Oluoch, J.. A survey of safe landing zone detection techniques for autonomous unmanned aerial vehicles. Intelligent Service Robotics, 17, 1-22.

[5] Guérin, J., Delmas, K., & Guiochet, J.. Certifying

Emergency Landing for Safe Urban UAV. 13th European Workshop on Dependable Computing.

[6] Loureiro, G., Dias, A., Martins, A., & Santana, J.. Emergency Landing Spot Detection Algorithm for Unmanned Aerial Vehicles. International Conference on Unmanned Aircraft Systems.

[7] Ramachandran, A.. Artificial Intelligence in Air Traffic Control: Advancing Safety, Efficiency, and Automation with Next-Generation AI Technologies. Journal of Air Transport Management, 109, 102383.

[8] Sundar, P. K. S., & Deka, P. C.. Spatio-Temporal Classification and Prediction of Land Use and Land Cover Change for the Vembanad Lake System, Kerala – a Machine Learning Approach. Aquatic Ecosystem Health & Management, 23, 421-431.

[9] Silva, L. P. e., Xavier, A. P. C., da Silva, R. M., and Santos, C. A. G.. "Modeling land cover change based on an artificial. International Journal of Applied Earth Observation and Geoinformation, 93, 102196.

[10] Tan, B., Lohan, E. S., Sun, B., & Yan, Z.. Improved Sensing and Positioning via 5G and mmWave radar for Airport Surveillance. IEEE Transactions on Aerospace and Electronic Systems, 57, 3619-3634.

[11] Wu, Q., Chen, J., Lu, Y., & Xu, J.. A Complete Automatic Target Recognition System of Low Altitude, Small RCS and Slow Speed Targets Based on Multi-Dimensional Feature Fusion. Sensors, 20, 5647.

[12] Matczak, G., & Mazurek, P.. Comparative Monte Carlo Analysis of Background Estimation Algorithms for Unmanned Aerial Vehicle Detection. Remote Sensing, 13, 1793.

[13] Sathaye, H., Schepers, D., Ranganathan, A., & Wetherall, D.. Wireless Attacks on Aircraft Instrument Landing Systems. USENIX Security Symposium.

[14] Ariante, G., & Del Core, G.. Unmanned Aircraft Systems: Current State, Emerging Technologies, and Future Trends. Inventions, 6, 64.

[15] Erturk, M. C., Hosseini, N., Jamal, H., Zhang, J., & Guvenc, I.. Requirements and Technologies Towards UAM: Communication, Navigation, and Surveillance. IEEE Vehicular Technology Magazine, 18, 44-54.

[16] Singh, V. K.. Assembly feature recognition and its application: A review. Frontiers in Mechanical Engineering, 9, 1241854.

[17] Velástegui-Montoya, A., Montalván-Burbano, N., Carrión-Mero, P., & Pérez-López, M.. Google Earth Engine: A Global Analysis and Future Trends. Remote Sensing, 15, 3675.

[18] Muñoz-Molina, L. J., Cazorla-Piñar, I., Dominguez Morales, J. P., & Ureña, J.. Real-time detection of uncalibrated sensors using neural networks. Software: Practice and Experience, 51, 2245-2264.

[19] Phoon, K. K.. Trustworthy data-centric geotechnics &. Computers and Geotechnics, 128, 103816.

[20] Sargiotis, D.. Advancing Civil Engineering with AI and Machine Learning: From Structural Health to Sustainable Development. Applied System Innovation, 7, 69.

[21] "Treatment episode data set: discharges (TEDS-D): concatenated, 2006 to 2009." U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies, August, 2013, DOI:10.3886/ICPSR30122.v2

Dr. M.M.Karthikeyan, "Optimizing Deep Image Super-Resolution Techniques for Low-Power Devices", Partners Universal International Innovation Journal (PUIIJ), Volume: 03, Issue: 03, May-June 2025, ISSN: 2583-9675.