iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: II Month of publication: February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77047

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

AeroShield: Advanced Drone Detection and Security Platform Using Deep Learning

Fathima Hashim[1], Mariyam Rubah[2], Mohammed Adhil Noushad[3], Muhammed Amre Ashaf[4], Ms Sharija P[5]
[1, 2, 3, 4]*Department of Computer Science and Engineering, Sree Narayana Guru College of Engineering and Technology, Kerala, India*
[5]*Assistant Professor, Department of Computer Science and Engineering, Sree Narayana Guru College of Engineering and Technology, Kerala, India*

Abstract: The usage of low-altitude drones has grown quickly, posing serious threats to security in sensitive and re- stricted locations. Drones are small and move quickly in complex areas, making it difficult for traditional surveillance systems to detect them. In order to achieve precise real-time detection on edge devices, this study provides an AI-based drone detection and forecasting system that uses a lightweight deep learning model tuned from YOLOv8n. While a time-series forecasting module forecasts future drone activity and creates risk heatmaps for proactive security planning, the system enhances detection performance through effective feature extraction and strong training techniques. It offers role-based monitoring, real-time alerts, and visualization through integration with web and mobile platforms. The technique is appropriate for practical drone surveillance applications since experimental findings demonstrate good detection accuracy with little computational cost.
Index Terms: Drone detection, YOLO, Deep learning, Edge computing, Forecasting, Security surveillance.

I. INTRODUCTION

Over the past decade, unmanned aerial vehicles (UAVs), also referred to as drones, have seen tremendous technological improvement and broad usage. Drones are very appealing for applications like aerial surveillance, environmental monitoring, traffic analysis, disaster response, infrastructure inspection, agriculture, and logistics because of their capacity to op- erate autonomously or semi-autonomously, as well as their reduced costs and enhanced maneuverability. Although these features have major positive social and economic effects, they also make drones vulnerable to abuse. Unauthorized drone incursions into critical or restricted airspaces, such as airports, military zones, industrial facilities, and public gatherings, pose major dangers to public safety, privacy, and possible criminal activity. The urgent need for dependable and efficient drone detection and monitoring systems that can function in real-world settings is highlighted by these developing concerns.Radar-based, radio-frequency (RF), and acoustic sensing methods are the mainstays of current drone detection methods. Even while these techniques have been effectively used in some surveillance situations, they have a number of intrinsic drawbacks when it comes to small, low-altitude, or commercially available drones. Lightweight drones have poor detection performance because radar sensors frequently have trouble detecting targets with a narrow radar cross-section. RF-based techniques are useless for autonomous or preprogrammed flights since they rely on constant signal transfer between the drone and its controller. In contrast, acoustic systems are less reliable in crowded or metropolitan environments because to their great sensitivity to environ- mental interference and background noise. Additionally, the scalability and adaptability of these conventional systems are often restricted by the need for specialized hardware, complicated calibration, and expensive deployment. Drone surveillance using visual data from cameras now has more options because to developments in computer vision and deep learning. In order to accurately detect objects in a variety of dynamic contexts, vision-based techniques use convolutional neural networks to automatically learn complicated spatial and semantic properties from photos and video streams. These systems have the advantages of easier deployment, less ex- pensive hardware, and versatility. Single-stage detectors have drawn the most interest among deep learning-based object identification models because of its great accuracy in real- time inference. For continuous monitoring tasks where quick response times are essential, these models are ideal.

Despite these benefits, there are a number of difficulties when using deep learning-based detection systems in real- world situations. The deployment of many cutting-edge mod- els on edge devices and platforms with limited resources is limited since they are computationally demanding and require high-performance GPUs. Furthermore, the majority of vision- based drone detection systems now in use are only capable of reactive detection, which means that alarms are only sent once a drone has entered the monitored region.

Because staff members are unable to foresee drone activity or plan suitable countermeasures in advance, the lack of predictive capabilities lowers the efficacy of security operations. Furthermore, the usefulness of many current solutions is further limited by the absence of integrated management modules including role- based access, alarm handling, and system feedback. This paper suggests an intelligent and integrated drone surveillance framework that combines system-level management, predic- tive forecasting, and lightweight real-time drone detection in order to get around these restrictions. In order to success- fully recognize small and low-altitude drones while keeping minimal computing complexity, the suggested system makes use of an optimized deep learning-based object detection model. To anticipate future intrusions and produce risk-aware insights, a time-series forecasting component examines past drone activity trends in addition to detection. By facilitating a transition from reactive monitoring to proactive surveillance, this predictive feature improves early warning and reaction capabilities.

The suggested framework provides a complete software architecture that includes online and mobile interfaces for real-time monitoring and warning distribution in addition to the essential AI components. Role-based access control enhances situational awareness and operational efficiency by enabling administrators, security staff, and users to engage with the system in accordance with assigned roles. The sys- tem attempts to offer a scalable, affordable, and deployable solution for contemporary drone surveillance requirements by combining detection, forecasting, and management features into a single platform. Real-world drone surveillance systems must have robustness and adaptability in addition to accuracy and processing efficiency. Variations in illumination, shadows, weather, and background clutter are examples of environ- mental elements that have a substantial impact on detection effectiveness. It can be challenging to tell small drones apart from birds or other flying objects since they frequently look as low-resolution objects with little visual signals. Models that can perform consistently and generalize well across a variety of operational situations are needed to address these issues. Because of this, training techniques including data augmentation, multi-scale feature learning, and improved loss functions are now crucial parts of contemporary drone de- tection frameworks.The timing aspect of aerial activities is another crucial factor in drone monitoring. Drone invasions frequently exhibit recurring patterns that are impacted by location, timing, and environmental variables. Nevertheless, the majority of current systems ignore temporal correlations in drone activity and regard detections as single occurrences. Systems can detect trends, recurrent intrusion zones, and time- based risk patterns by including temporal analysis. By enabling security staff to better deploy resources and react before an attack worsens, forecasting future drone activity based on past detection data can greatly increase preparation.

For drone detection technologies to be practically usable, system-level integration is also essential. Without methods for user interaction, warning distribution, and visualization, a detection model by itself is inadequate. Role-based access management, automatic alert systems, and real-time dash- boards increase situational awareness and speed up response times. Additionally, the ability to convert insights produced by AI models into practical actions is ensured by integrating detection and forecasting outputs with software platforms. The gap between algorithmic performance and operational efficacy is filled by such integration. For drone surveillance systems to be widely used, scalability and deployability are two more issues that need to be resolved. Due to technology limitations, network slowness, or operational complexity, solutions created for lab conditions frequently fail when implemented in real- world circumstances. More flexibility and cost effectiveness are provided by software-based systems that use lightweight models and conventional computing infrastructure. Without re- quiring major hardware changes, these systems can be readily updated, deployed in various places, and adjusted to chang- ing threat scenarios. Maintaining dependable performance in diverse deployment situations is a major difficulty in drone surveillance. Surveillance systems may need to function in industrial zones, open rural areas, metropolitan areas with dense infrastructure, or close to vital facilities, each of which has distinct visual traits and interference sources. The detection process is made more difficult by variations in camera posi- tioning, resolution, viewing angles, and background motion. In order to ensure constant detection performance under a variety of operational restrictions, a strong surveillance system must be able to adjust to these environmental fluctuations with- out requiring significant manual reconfiguration. Furthermore, intelligent monitoring systems that can function constantly with little human intervention are required due to the growing number of autonomous and semi-autonomous drones. Manual live video stream monitoring is time-consuming and prone to human mistake, especially in situations involving long-term or high-risk surveillance. By continuously processing visual data, recognizing possible hazards, and producing alerts in real time, automated detection and analysis lessen this strain. By incorporating learning-based models, systems can contin- uously improve their detection and analysis skills as more data becomes available. Drone surveillance is growing more and more concerned with ethical and legal issues in addition to operational effectiveness. In order to ensure that acquired data is handled responsibly and accessible only by authorized individuals, systems intended for airspace surveillance must strike a balance between security requirements and privacy preservation. Maintaining confidence and adhering to regulations requires transparent system functioning, secure data storage, and role-based access control.

Modern surveillance frameworks can support both security goals and responsible system deployment by implementing controlled data handling and structured access procedures.

Overall, by fusing precision, effectiveness, and predictive intelligence, the suggested method tackles major issues with existing drone detection systems. It contributes to safer and more secure aerial environments because of its software-based design, lightweight models, and modular architecture, which make it appropriate for deployment in real-world scenarios like restricted airspace monitoring, smart city surveillance, and critical infrastructure protection.

II. RELATED WORKS

A. Vision-Based Drone Detection Using YOLO Frameworks

Because of the YOLO (You Only Look Once) family of deep learning models' strong detection accuracy and real- time performance, vision-based drone detection has been thor- oughly investigated in recent works. Lightweight YOLO varia- tions like YOLOv5, YOLOv7, and YOLOv8 have been shown by researchers to be successful in identifying unmanned aerial aircraft in surveillance situations. In order to quickly identify drones in dynamic surroundings, our models use convolutional neural networks to extract spatial characteristics from photos and videos. However, current YOLO-based methods frequently have trouble identifying small, low-altitude drones, particu- larly in cluttered backdrops like trees, buildings, or birds. Furthermore, a lot of high-accuracy models need strong GPU hardware, which restricts their use on low-resource systems or edge devices.

B. Lightweight and Optimized Models for Small Drone De- tection

Several studies have suggested efficient and lightweight models designed for small object identification in order to overcome the shortcomings of traditional YOLO designs. To increase detection accuracy while lowering computing cost, methods such grouped convolutions, attention mechanisms, feature pyramid upgrades, and modified backbones have been devised. Methods that use multi-scale feature fusion, Bottle- neckCSP structures, and GhostNet backbones have demon- strated significant gains in the detection of small drones with lower GFLOPs and fewer parameters. Despite these develop- ments, many systems remain reactive rather than proactive in real-world security applications because they only concentrate on detection and lack forecasting or prediction capabilities.

C. Drone Activity Prediction and Time-Series Forecasting

Recent studies have started investigating predictive mod- eling methods to foresee drone movements and potential intrusions in addition to detection. To forecast future activity patterns, time-series forecasting models such Gated Recurrent Unit (GRU) networks and Long Short-Term Memory (LSTM) have been used to sequential drone detection data. To deter- mine the probability of drone recurrence in particular areas or time periods, these models examine temporal dependencies in past data. Forecasting-based methods enhance readiness and early warning, but they are frequently used separately from detection systems and do not seamlessly integrate with operational dashboards and real-time monitoring pipelines.

D. System-Level Integration and Surveillance Platforms

Numerous research have suggested integrated surveillance frameworks that combine alarm systems, monitoring dash- boards, and detection algorithms. Web-based interfaces are frequently used by these platforms to manage and visualize detection findings. However, mobile integration, role-based access control, and modular architecture are absent from the majority of current solutions. Additionally, it is still difficult to synchronize detection, prediction, and alarm modules in real-time, particularly when operating in dispersed or edge- based contexts. A unified, lightweight, and predictive drone surveillance framework that combines detection, forecasting, and system administration into a single platform is necessary in light of these deficiencies.

III. CONCLUSION FROM LITERATURE SURVEY

According to the literature review, a lot of research has been done to enhance drone detection accuracy and real- time performance utilizing both vision-based and sensor-based methods. Although radar, acoustic, and radio-frequency meth- ods have been extensively investigated, their efficacy is fre- quently restricted when identifying small, low-altitude drones in challenging circumstances. Additionally, these techniques rely heavily on specialized hardware and are vulnerable to environmental factors, noise, and interference, which limits their scalability and dependability in real-world applications. In real-time drone identification, vision-based deep learning techniques—especially those based on convolutional neural networks and YOLO architectures—have proven to perform better.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

Recent research demonstrates how attention mecha- nisms, improved feature fusion techniques, and lightweight and efficient YOLO variations can improve small-drone de- tection while lowering computational overhead. Despite these developments, many current models still have false detections, particularly when it comes to differentiating drones from birds or other flying objects, and they frequently need sizable, well selected datasets in order to maintain reliable performance. Additionally, the survey shows that the majority of current drone surveillance systems lack predictive capabilities and are solely concerned with detection. Despite the fact that predictive intelligence is essential for proactive threat man- agement, very few studies take into account temporal analysis or forecasting of drone activities. The operational utility of many suggested solutions is further limited by the frequent neglect of system-level integration, which includes warning systems, role-based access control, and real-time visualization. The literature as a whole reveals a glaring research deficit in the creation of integrated drone surveillance frameworks that incorporate comprehensive system management, lightweight real-time detection, and predictive forecasting into a single platform. These results highlight the need for software-based, intelligent solutions that can provide early warning, accurate detection, and scalable deployment for practical airspace se- curity applications.

IV. SYSTEM ARCHITECTURE

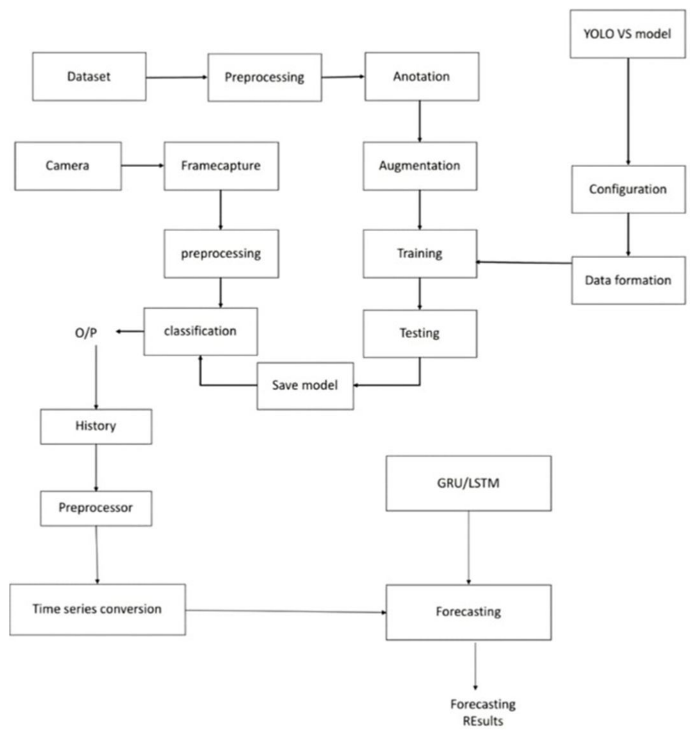


Fig. 1. System Architecture of the Proposed AeroShield Drone Detection and Forecasting Framework

Data collecting from two main sources—pre-collected datasets and real-time camera inputs—is the first step in the AeroShield system architecture. Preprocessing is used to the dataset in order to eliminate noise, standardize image quality, and get samples ready for annotation. Data augmentation techniques are used to further improve the robustness and generality of annotated data. After appropriate setup and data formatting, the YOLO-based detection model is trained using these generated examples. Before being sent to the trained detection model, real-time video streams obtained from cameras are simultaneously processed through frame capture and preprocessing phases. The model generates real- time detection outputs by classifying and localizing drones in incoming frames. To guarantee effective deployment and consistency across detection tasks, the trained model is saved and utilized again for inference.

The forecasting pipeline uses the detection outputs, which are continuously recorded and saved as historical data. To capture drone activity patterns over time, this historical data is preprocessed and transformed into time-series data. Following processing, the time-series data is input into GRU/LSTM- based forecasting models, which use historical detection trends to forecast future drone movements and possible intrusion threats.

Lastly, the forecasting module produces predictive outcomes that facilitate proactive decision-making and early warning. The AeroShield architecture converts traditional re- active drone monitoring into an intelligent and predictive aerial surveillance system that can function effectively on common computing platforms by fusing real-time detection with temporal forecasting.

V. RESULTS AND DISCUSSIONS

A combination of real-world and publicly accessible drone datasets, including difficult surveillance scenarios including small drone sizes, low-altitude flights, cluttered backgrounds, and varied illumination conditions, were used to assess the per- formance of the proposed AeroShield system. These datasets were chosen to represent real-world operational settings where precise drone detection is challenging. To determine the overall efficacy of the suggested framework, the study concentrated on important criteria such as detection accuracy, computational efficiency, forecasting reliability, and system-level integration. According on experimental data, the enhanced YOLO-GCOF detection model significantly outperforms baseline YOLOv8n models,achieving a mean Average Precision (mAP@50) of roughly 91.5%.

Better depiction of small and far-off drones is made possible by the addition of the GI-DGCST backbone, which greatly improves feature extraction while keeping a lightweight frame- work. Furthermore, the CSA-HSFPN neck enhances multi- scale feature fusion, enabling the model to capture contextual data at various spatial resolutions. Bounding box localization accuracy is further enhanced by the application of Focaler- SIoU loss, especially for fast-moving drones and distant tar- gets.AeroShield exhibits robust computing performance that is appropriate for real-time deployment. When compared to traditional detection designs, the optimized model reduces computational complexity (GFLOPs) by about 50% and pa- rameter count by over 60%. Without compromising detection accuracy, these reductions allow real-time inference on edge devices and resource-constrained systems. The findings demonstrate that the suggested model successfully strikes a compromise between efficiency and performance, making it useful for applications involving continuous surveillance. Overall, the experimental results show that by combining high detection accuracy, lightweight computation, and predictive intelligence, AeroShield effectively addresses major shortcom- ings of current drone surveillance systems. Even though the system functions dependably in most situations, it may be made even better by adding extreme weather events to the training dataset and using segmentation-based refinement to increase boundary precision. These outcomes confirm that AeroShield is a reliable and expandable solution for intelligent aerial intrusion detection and monitoring in practical settings.

VI. CONCLUSION

AeroShield, a lightweight and sophisticated aerial intrusion detection and forecasting system created to handle the escalat- ing security issues brought on by unauthorized drone activity, was introduced in this study. Real-time drone recognition and proactive incursion prediction are made possible by the system's integration of a time-series forecasting module with an optimized YOLO-GCOF-based detection framework. For small and low-altitude drones, the employment of effective feature extraction, multi-scale fusion approaches, and im- proved loss functions greatly increases detection accuracy while preserving minimal processing overhead appropriate for edge deployment. By examining past drone activity patterns and producing early warnings through danger maps and alerts, the integration of LSTM/GRU-based forecasting improves situational awareness in addition to detection. By converting conventional reactive surveillance systems into proactive de- fense mechanisms, this predictive capability enables security staff to foresee possible dangers and react more skillfully. The Admin, Security, User, and Drone Owner modules that make up the modular system architecture guarantee well-organized data administration, role-based access control, and smooth coordination between web and mobile platforms.Additionally, AeroShield's design philosophy places a strong emphasis on extensibility and adaptability, allowing the system to develop in tandem with new drone technologies and changing threat scenarios. The software-centric approach makes it simple to expand datasets, update models, and incorporate sophisti- cated learning methods including segmentation, spatiotempo- ral modeling, and adaptive risk assessment. AeroShield offers a versatile architecture that can handle extensive surveillance infrastructures by facilitating deployment across dispersed edge nodes and centralized monitoring platforms. Because of its versatility, the system is well-positioned for practical imple- mentation in vital applications like border monitoring, airport security, and smart city airspace management. All things considered, AeroShield presents a software-based, scalable solution that connects intelligent forecasting and high-accuracy drone detection without the need for specific hardware. The suggested strategy provides a useful and affordable framework for contemporary airspace surveillance and establishes a solid basis for upcoming developments in intelligent drone monitor- ing, predictive security systems, and practical implementation in delicate and restricted areas.

REFERENCES

[1] F. N. M. Zamri, T. S. Gunawan, S. H. Yusoff, A. A. Alzahrani, A. Bramantoro, and M. Kartiwi, "Enhanced Small Drone Detection Using Optimized YOLOv8 with Attention Mechanisms," IEEE Access, vol. 12, pp. 1–12, 2024, doi: 10.1109/ACCESS.2024.YOLOV8.

[2] X. Tu, C. Zhang, H. Zhuang, S. Liu, and R. Li, "Fast Drone Detection with Optimized Feature Capture and Modeling Algo- rithms," IEEE Access, vol. 12, pp. 1–10, 2024, doi: 10.1109/AC- CESS.2024.OPTIDRONE.

[3] K. K. Akash and U. Kuppusamy, "Drone Detection Using YOLOv5 with GhostNet Backbone and Adaptive Fourier Neural Operator (AFNO 2D)," IEEE Access, vol. 13, pp. 1–9, 2025, doi: 10.1109/AC- CESS.2025.AFNO2D.

[4] K. Ogawa, D. Tsagaanbayar, and R. Nakamura, "ISAR Imag- ing for Drone Detection Based on Backprojection Algorithm Us- ing Millimeter-Wave Fast Chirp Modulation MIMO Radar," IE- ICE Communications Express, vol. 13, no. 5, pp. 1–7, 2024, doi: 10.1587/comex.2024.ISARDRONE.

[5] A. Pandat, P. Rajasekhar, G. Vinod, and R. Shukla, "Strategies for Improved Out-of-Distribution Detection in Drone vs. Bird Classifica- tion," Procedia Computer Science, vol. 240, pp. 1200–1210, 2025, doi: 10.1016/j.procs.2025.04.085.

[6] B. Srinivasa, S. P. Kumar, and I. A. Wani, "Realtime Drone Detection Using YOLOv8 and TensorFlow.JS," Journal of Engineering Sciences, vol. 15, no. 2, pp. 101–110, 2024, doi: 10.1016/j.jes.2024.02.015.

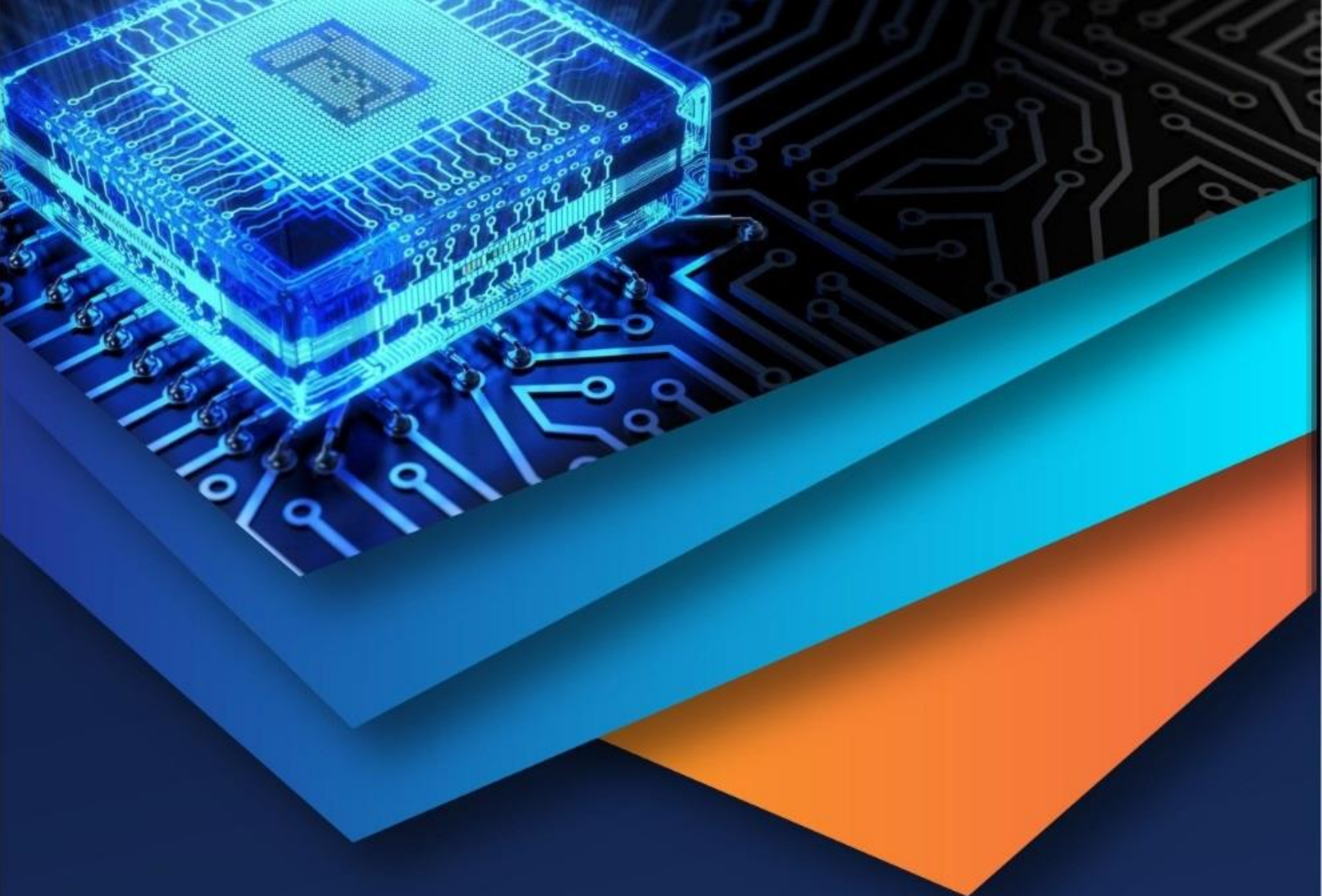
[7] S. Glu¨ge, M. Nyfeler, A. Aghaebrahimian, N. Ramagnano, and C. Schu¨pbach, "Robust Low-Cost Drone Detection and Classification Using Convolutional Neural Networks in Low SNR Environments," IEEE Journal of Radio Frequency Identification, vol. 8, no. 3, pp. 210–218, 2024, doi: 10.1109/JRFID.2024.0123456.

[8] H. Lee, S. Han, J.-I. Byeon, S. Han, R. Myung, J. Joung, and J. Choi, "CNN-Based UAV Detection and Classification Using Sensor Fusion," IEEE Access, vol. 11, pp. 23000–23012, 2023, doi: 10.1109/AC- CESS.2023.2300123.

[9] D. Chauhan, H. Kagathara, H. Mewada, S. Patel, S. Kavaiya, and
G. Barb, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies," IEEE Access, vol. 13, pp. 4500– 4515, 2025, doi: 10.1109/ACCESS.2025.0450015.

[10] I. Atik, "CB-YOLOv5: Enhancing Drone Detection with BottleneckCSP and Cross Convolution for Improved Performance," Journal of Radiation Research and Applied Sciences, vol. 16, no. 1, pp. 50–58, 2023, doi: 10.1016/j.jrras.2023.01.005.

[11] W. Yu and K. Mo, "YOLO-GCOF: A Lightweight Low-Altitude Drone Detection Model," IEEE Access, 2025, doi: 10.1109/AC- CESS.2025.3553477.



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY