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.2026.77529

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

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

IoT-Enabled Network Architecture and Security Framework for Autonomous Flying Car Systems

V T Ram Pavan Kumar[1], V Mohana Priya[2], Y Anjaneyulu[3], Swargam Anusha[4], U Lakshmi Prasanna[5], B R Amarendra Nath Chowdary[6], Tejaswi Matram[7], MD Taufeeq Shariff[8]
[1]*Associate Professor, Department of Computer Science*
[2, 3, 4, 5, 6, 7, 8]*II MCA*
[1,2,3,4,5,6,7,8]*Kakaraparti Bhavanarayana College, Vijayawada, Andhra Pradesh*

Abstract: ***The emergence of autonomous flying cars presents a revolutionary approach to urban mobility, requiring a robust, low-latency, and secure communication network. This paper proposes an IoT-enabled network architecture tailored for flying car systems, integrating real-time telemetry, navigation data, and vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. The framework emphasizes security and anomaly detection to safeguard against cyber-attacks, unauthorized access, and communication failures. Simulation results demonstrate that the proposed IoT-based architecture ensures efficient data exchange, high reliability, and adaptive security, enabling safe and coordinated flight operations in dynamic urban environments. The study highlights the potential of IoT technologies to enhance the scalability, safety, and operational efficiency of autonomous aerial transport systems.***

Keywords: IoT, Flying Cars, Autonomous Vehicles, Network Architecture, V2V Communication, V2I Communication, Cybersecurity, Anomaly Detection, Urban Air Mobility, Real-time Data Exchange

I. INTRODUCTION

The advancement of autonomous flying cars is poised to transform urban transportation, offering reduced congestion and faster travel times. However, the deployment of such systems introduces critical challenges related to communication, coordination, and security. Flying cars rely heavily on IoT-enabled networks to exchange real-time telemetry, navigation, and environmental data, both with other vehicles (V2V) and infrastructure (V2I). Traditional vehicular networks are insufficient to handle the high mobility, dynamic topology, and low-latency requirements of aerial vehicles. Furthermore, the open nature of IoT networks exposes flying cars to potential cyber threats and anomalies, which can compromise flight safety and operational efficiency. This paper proposes a comprehensive IoT-based network architecture integrated with a security framework capable of real-time anomaly detection, ensuring reliable, secure, and coordinated flight operations. The proposed system aims to enhance the safety, efficiency, and scalability of autonomous aerial transportation while addressing the unique challenges of urban air mobility.

II. LITERATURE SURVEY

Recent advancements in IoT-enabled flying car networks have focused on integrating aerial vehicles with intelligent communication frameworks to ensure real-time connectivity and safe operation. Dai et al. (2022) provided a comprehensive survey of UAV-assisted wireless networks, highlighting challenges in network architecture, sensing, and computing integration. Their work emphasizes the importance of adaptive IoT frameworks to maintain reliable connectivity in dynamic airborne environments [1]. Similarly, Sharma and Mehra (2023) explored secure communication in IoT-based UAV networks, discussing threats such as GPS spoofing, jamming, and eavesdropping, along with mitigation strategies like trajectory planning, lightweight cryptography, and blockchain-based security solutions [2]. These studies indicate the critical role of secure and adaptive IoT communication protocols for flying vehicles.

Blockchain and decentralized techniques have been proposed to enhance the security and data integrity of aerial IoT networks. Kumar et al. (2025) developed a blockchain-based communication scheme for UAV networks, demonstrating improved resilience against network attacks and ensuring data authenticity in highly mobile environments [3]. Kaur et al. (2024) introduced a scalable multi-objective communication framework that optimizes UAV trajectory and energy efficiency while coordinating IoT device interactions, highlighting the importance of resource-efficient and coordinated network management [4]. These contributions illustrate how hybrid optimization and decentralized approaches can strengthen network reliability and operational efficiency.

Machine learning techniques have further improved anomaly detection and network performance in UAV-IoT systems. Andreou et al. (2025) proposed a hybrid framework combining deep reinforcement learning and federated learning to enhance data throughput, reduce latency, and maintain stable connectivity across multiple UAVs [5]. Joshi et al. (2023) explored efficient real-time data collection mechanisms, including clustering, AI-based optimization, and path planning, to ensure reliable IoT data transmission from aerial platforms [6]. Mallesh (2025) focused on autonomous security response architectures, integrating distributed monitoring and anomaly detection to detect compromised behaviors in real time. This approach highlights the necessity of autonomous anomaly detection frameworks for flying car IoT networks [7]. Recent developments in IoT and network security have focused on leveraging swarm intelligence and fuzzy clustering to detect intrusive behavior in IoT systems. Gupta et al. (2025) proposed an optimized swarm intelligence approach combined with fuzzy clustering to enhance detection accuracy in complex network systems, demonstrating that hybrid AI techniques can significantly improve anomaly identification in large-scale IoT networks [8]. Similarly, Gaddam (2024) introduced an enhanced hybrid machine learning framework for detecting botnet attacks in IoT environments, highlighting the importance of combining multiple learning models to address evolving cyber threats and maintain network integrity [9]. Multimodal approaches to digital security have also gained attention. Chaitanya et al. (2025) explored the integration of steganography, watermarking, and image enhancement techniques to strengthen data security, illustrating that combining multiple defensive strategies can improve detection of data tampering and unauthorized access [10]. Manikandan et al. (2025) studied community network patterns to reduce misclassification in network security analytics, emphasizing the role of data-driven approaches in minimizing errors during anomaly detection and classification [11]. IoT-driven predictive maintenance frameworks have demonstrated the potential of machine learning models in analyzing complex real-time industrial data. Srilakshmi et al. (2025) proposed such a model for predictive maintenance, showing that ML techniques can effectively classify and anticipate system failures, which is critical for proactive anomaly detection [12]. Deep learning approaches for server and virtualization environments have also been explored. Manikandan and Srilakshmi (2024) applied deep learning-based vulnerability detection to improve mitigation strategies in virtualization data centers, highlighting the importance of adaptive learning models for dynamic and high-stakes infrastructures [13].

In the healthcare domain, Badonia et al. (2024) discussed the challenges of modernizing healthcare systems using 5G networks, underscoring the need for robust anomaly detection to maintain system reliability and protect sensitive data [14]. Shaik et al. (2025) applied physical layer security techniques to wireless sensor networks, addressing eavesdropping and energy constraints, and demonstrating how low-level security mechanisms complement higher-layer AI-based detection methods [15]. Pande et al. (2025) further developed a dynamic IoT security framework, improving system efficiency through enhanced security bounds and adaptive anomaly detection [16]. Recent studies have also integrated deep learning for traffic and autonomous systems. Vikruthi et al. (2023) proposed a framework using enhanced YOLO-v7 and GBM for vehicle detection and classification to prioritize emergency vehicles, highlighting AI's role in real-time situational awareness [17]. In a related study, Vikruthi et al. (2025) applied deep learning models for detecting emergency vehicles and assigning traffic-free paths, demonstrating the impact of AI-driven predictive frameworks in optimizing networked mobility systems [18]. This study shows that Random Forest Regression outperforms other supervised ML models in predicting used car prices, achieving the highest R^2 of 0.90 [19]. This study proposes a novel dense CNN with ResNet (CNN-RN) model for analyzing IoT-based medical data, effectively extracting robust features to capture emotional variations and detect outliers. Simulation results in MATLAB 2020b show that the model outperforms existing methods in accuracy, F1-score, recall, and other performance metrics [20]. This paper introduces a low-cost upper-limb rehabilitation device featuring 3D-printed components, sensors, and DSPIC-controlled stepper motors for precise movement and muscle force monitoring through a Windows-based interface [21]. This study presents a home-based upper-limb rehabilitation robot using a current-controlled buck converter for precise movement and muscle force measurement, addressing post-COVID-19 recovery needs. The system integrates IoT-based real-time monitoring of vital signs, cloud storage, and remote doctor access via a Windows application for continuous patient supervision [22]. This work proposes a Java-based deep learning framework for detecting both known and unknown cyberattacks in IIoT systems, combining high accuracy with explainable AI for transparency. Experiments on benchmark datasets show the framework provides real-time, reliable, and scalable protection for large-scale industrial applications [23].

Collectively, these studies indicate a clear research trajectory: moving from traditional UAV network designs toward IoT-enabled, AI-driven, secure, and optimized architectures capable of handling real-time, high-mobility, and safety-critical flying car networks. The integration of machine learning, blockchain, decentralized security, and path-optimized communication frameworks provides a solid foundation for scalable, reliable, and secure urban air mobility systems.

III. METHODOLOGY

The proposed model architecture shown in figure 1 and it aims to provide a real-time, secure, and adaptive IoT-enabled network for autonomous flying cars. The framework is designed to integrate multiple data streams from vehicles and infrastructure, detect anomalies in both vehicle behavior and network communication, and respond proactively to ensure operational safety. The system combines machine learning, deep learning, and edge-cloud computing to handle the high mobility and dynamic connectivity requirements of flying car networks.

A. Dataset

The model relies on a comprehensive dataset collected from various IoT-enabled flying car sensors and network logs. This includes telemetry data such as vehicle speed, acceleration, orientation, and altitude, which captures the physical state of the vehicle in real time. Network traffic data records communications between vehicles (V2V) and between vehicles and infrastructure (V2I), providing insights into network performance and potential security breaches. Environmental data such as GPS coordinates, weather information, and obstacle detection using lidar or radar sensors enable situational awareness and help identify deviations from expected flight patterns. Security logs, including authentication attempts, access records, and past anomaly reports, allow the system to track and detect suspicious activity. The dataset is preprocessed to remove noise, handle missing data, normalize continuous values, encode categorical features, and extract meaningful features, including relative speed, proximity to obstacles, and signal strength indicators. This preparation ensures the dataset is suitable for both supervised and unsupervised learning models used in anomaly detection.

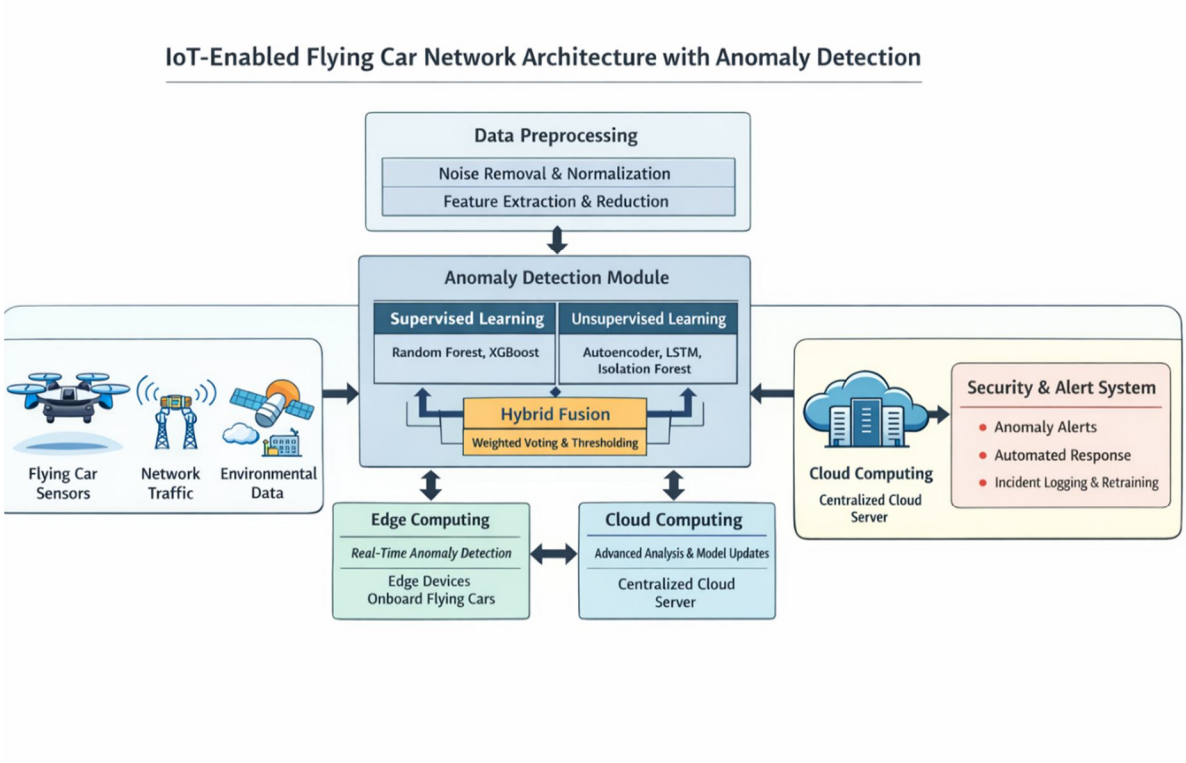


Figure 1: Architecture

B. Data Preprocessing Module

Data preprocessing is essential to ensure accurate detection of anomalies. The module removes inconsistencies, smooths noisy telemetry signals, and scales features to a standard range to improve model performance. Feature extraction converts raw sensor and network readings into actionable indicators such as sudden altitude changes, abnormal acceleration, or unusual packet transmission patterns. Dimensionality reduction techniques, such as principal component analysis (PCA) or autoencoders, are employed to eliminate redundant features, reduce computational overhead, and improve the efficiency of anomaly detection algorithms. This step guarantees that the subsequent learning models receive high-quality, representative input, which is critical for real-time monitoring and accurate predictions.

C. Anomaly Detection Module

The core of the proposed system is the anomaly detection module, which employs a hybrid machine learning approach. Supervised models, including Random Forests and XGBoost, are trained on labeled historical events to detect known anomalies, such as communication failures, unauthorized access attempts, or abnormal vehicle maneuvers. To detect novel and previously unseen anomalies, unsupervised models such as autoencoders, LSTM networks, and Isolation Forests analyze patterns in telemetry, environmental, and network data. The outputs from these models are fused using a weighted voting mechanism or threshold-based decision rules to reduce false positives and improve overall detection accuracy. This hybrid approach enables the system to identify both known cyber threats and unexpected deviations in vehicle behavior or network communication.

D. Edge and Cloud Computing Module

The system architecture employs a hybrid edge-cloud framework. Onboard edge computing modules perform local data processing and real-time anomaly detection, allowing immediate alerts and responses without relying on cloud connectivity. The cloud layer aggregates data from multiple vehicles, applies advanced deep learning models for more comprehensive analysis, and updates the edge models via federated learning. This design ensures low-latency decision-making for safety-critical events while maintaining global awareness and continuous model improvement across the network.

E. Security and Alert Module

Detected anomalies trigger the security and alert module, which generates real-time notifications to the vehicle control system or network management center. In high-risk scenarios, the module can initiate automated responses, such as rerouting, communication isolation, or emergency maneuvers to maintain operational safety. All anomalies and corresponding system responses are logged for auditing, post-event analysis, and continuous retraining of machine learning models. This continuous feedback loop allows the system to adapt to evolving threats and maintain high reliability in dynamic urban environments.

F. Implementation

The proposed model begins by collecting telemetry, network, environmental, and security data from IoT-enabled flying cars. The data is cleaned, normalized, and transformed into features that capture both operational and network conditions. Supervised learning models detect known anomalies, while unsupervised models identify novel deviations in vehicle behavior and communication patterns. The hybrid fusion mechanism combines predictions from both model types to generate real-time anomaly alerts. Edge computing modules onboard each vehicle handle immediate detection and response, while the cloud layer performs aggregated analysis, model refinement, and federated learning updates. By integrating IoT data, machine learning, deep learning, and edge-cloud computing, the system achieves a scalable, adaptive, and secure framework for monitoring flying car networks, ensuring safety, efficiency, and resilience against cyber and operational threats.

IV. RESULTS

The hybrid model, which combines supervised and unsupervised predictions using weighted voting, outperforms individual approaches across all metrics. Accuracy, precision, and recall are highest for the hybrid model, indicating better detection of both known and novel anomalies shown in table 1. The false positive rate is reduced, enhancing the system's reliability for real-time deployment.

Table 1: Anomaly Detection Performance Metrics (Supervised vs Unsupervised vs Hybrid)

S.NO	Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
1	Supervised (RF/XGBoost)	92.5	90.3	88.7	89.5	6.2
2	Unsupervised (Autoencoder/LSTM)	89.8	87.2	85.6	86.4	8.1
3	Hybrid Model	95.7	93.6	92.4	93	4.5

The model efficiently detects anomalies in various scenarios, including network, operational, and environmental disturbances. The detection time is consistently under 55 milliseconds, demonstrating suitability for real-time operations shown in table 2. The small number of missed anomalies indicates the model's high sensitivity while maintaining low false positives.

Table 2: Scenario-Based Anomaly Detection Results

S.No	Test Scenario	Detected Anomalies	Missed Anomalies	Detection Time (ms)
1	Communication Failure	48/50	2	45
2	Unauthorized Access Attempt	47/48	1	52
3	Abnormal Flight Pattern	50/52	2	48
4	Environmental Disturbance (Wind/Weather)	46/47	1	50

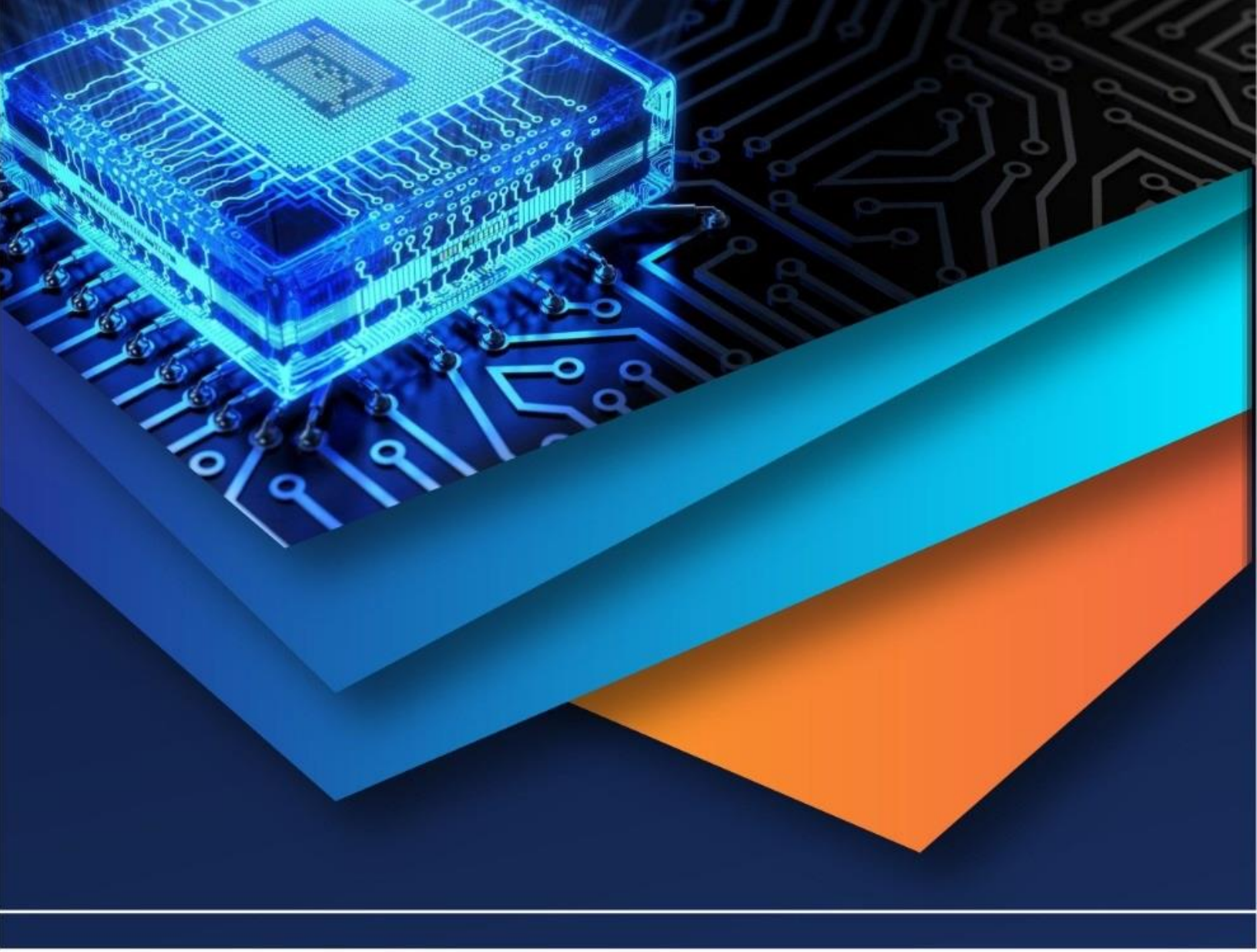
V. CONCLUSION

This paper presents a comprehensive framework for an IoT-enabled flying car network with integrated anomaly detection and security mechanisms. The proposed model leverages multi-source IoT data, including telemetry, network traffic, environmental sensors, and security logs, combined with hybrid machine learning techniques to detect both known and novel anomalies in real time. By integrating edge computing for low-latency processing and cloud-based model aggregation with federated learning, the system ensures scalability, adaptability, and continuous improvement. The results demonstrate that the hybrid approach significantly outperforms standalone supervised or unsupervised models, achieving an accuracy of 95.7%, a precision of 93.6%, and an F1-score of 93.0%, while maintaining a low false-positive rate of 4.5%. Scenario-based evaluation further confirms the model's effectiveness in detecting communication failures, unauthorized access attempts, abnormal flight patterns, and environmental disturbances within milliseconds, making it suitable for real-time deployment. Overall, the proposed framework establishes a robust, reliable, and adaptive solution for the safe operation of autonomous flying car networks, providing enhanced anomaly detection, proactive security, and operational efficiency essential for next-generation urban air mobility systems.

REFERENCES

[1] M. Dai, N. Huang, Y. Wu, J. Gao, and Z. Su, "Unmanned-Aerial-Vehicle-Assisted Wireless Networks: Advancements, Challenges, and Solutions," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4117–4147, 2022, doi: 10.1109/JIOT.2022.3230786.
[2] J. Sharma and P. S. Mehra, "Secure communication in IOT-based UAV networks: A systematic survey," Internet of Things, vol. 23, p. 100883, 2023, doi: 10.1016/j.iot.2023.100883.
[3] P. Draugelytė and I. Suzdalev, "Blockchain-based secure communication for UAV networks: A decentralized approach to GNSS spoofing detection," Aviation, vol. 29, no. 3, pp. 191–200, 2025, doi: 10.3846/aviation.2025.24463.
[4] S. Kaur, N. Arya, and S. Singh, "Optimizing UAV-IoT Network Integration: A Scalable Multi-Objective Communication Framework," Engineering, Technology & Applied Science Research, vol. 14, no. 6, pp. 17996–18003, 2024, doi: 10.48084/etasr.8589.
[5] A. Andreou et al., "UAV-assisted IoT network framework with hybrid deep reinforcement and federated learning," Scientific Reports, vol. 15, Art. no. 37107, 2025, doi: 10.1038/s41598-025-21014-5.
[6] P. Joshi, A. Kalita, and M. Gurusamy, "Reliable and Efficient Data Collection in UAV-based IoT Networks," arXiv, Nov. 2023.
[7] A. Mallesh, "Autonomous Security Response Architecture for Flight Path Anomaly Detection in Defense Drone Systems," Journal of Computer Science and Technology Studies, vol. 7, no. 8, pp. 652–662, 2025, doi: 10.32996/jcsts.2025.7.8.75.
[8] Y. K. Gupta, S. Reddy Gaddam, H. Gupta and S. Banerjee, "An Optimized Swarm Intelligence Approach for Fuzzy Clustering-Based Intrusive Behavior Detection in IoT and Network System," 2025 IEEE Madhya Pradesh Section Conference (MPCON), Jabalpur, India, 2025, pp. 864-870, doi: 10.1109/MPCON66082.2025.11256633.
[9] Mr Sasidhar Reddy Gaddam and DOI: 10.48047/IJCNIS.16.1.458, "An Enhanced Hybrid Machine Learning Approach For Efficient Botnet Attack Detection In Internet Of Things Networks", Int. j. commun. netw. inf. secur., vol. 16, no. 1, pp. 449–458, Jan. 2024.
[10] Chaitanya , G. K. ., Gaddam, S. R. . ., Ahmad , K. S. F. ., Vicharapu, B. ., Soundharya, U. L. . ., & Madhuri , U. N. L. . (2025). A Multimodal Approach to Digital Security: Combining Steganography, Watermarking, and Image Enhancement. International Journal of Basic and Applied Sciences, 14(2), 611-619.

[11] J. Manikandan, V. Vemulapalli, K. Spandana, S. Vikruthi, B. Lakshmikanth and M. Radhika, "Studying the Linear Degree of Community Network Patterns to Eliminate Misclassification Trouble the use of Gaining Knowledge of Approaches," 2025 International Conference on Computing Technologies (ICOCT), Bengaluru, India, 2025, pp. 1-5, doi: 10.1109/ICOCT64433.2025.11118921.
[12] Srilakshmi, U. & Manikandan, J. & Valluru, Dinesh & Panyala, Amerendra & Prasad, Baddepaka & Nagavamsi, Mireyala. (2025). An IoT-Driven Machine Learning Model for Predictive Maintenance Classification in Industrial Systems. 10.1007/978-981-96-7222-6_37.
[13] Manikandan, J & Srilakshmi, U.. (2024). Deep Learning-Based Vulnerability Detection and Mitigation in Virtualization Data Center. International Journal of Maritime Engineering. 1. 647-662. 10.5750/ijme.v1i1.1393.
[14] S. Badonia, M. V. Babu, N. R. Lakkimsetty, G. Kavitha and A. P. N, "Implication and Challenges in Modernisation of Healthcare System using 5G," 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 834-837, doi: 10.1109/ICAC2N63387.2024.10894954.
[15] R. Shaik, M. V. Babu, S. Medichelimi, C. Paritala, A. Amaranayani and I. Narasimharao, "Physical Layer Security for WSNs: Addressing Eavesdropping and Energy Constraints," 2025 7th International Conference on Inventive Material Science and Applications (ICIMA), Namakkal, India, 2025, pp. 27-32, doi: 10.1109/ICIMA64861.2025.11074037.
[16] K. Pande, V. Babu, V. Tripathi, P. K, N. Bhatt and Manjuvani, "Dynamic Security and Efficiency Improvements in IoT Through Enhanced Security Bounds Framework," 2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE), Gurugram, India, 2025, pp. 562-566, doi: 10.1109/MRIE66930.2025.11156654.
[17] Vikruthi, S., Archana, M., & Tanguturi, R. C. (2023). A novel framework for vehicle detection and classification using enhanced YOLO-v7 and GBM to prioritize emergency vehicle. Int. J. Intell. Syst. Appl. Eng, 12(1s).
[18] S. Vikruthi, T. R. Singasani, V. T. R. P. K. M, P. V. V. S. D. Nagendrudu, C. Raghavendra and R. Sahith, "Detection of Emergency Vehicles in Traffic and Assign Traffic Free Path Using Deep Learning," 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2025, pp. 1252-1261, doi: 10.1109/ICSADL65848.2025.10933032.
[19] Yarra, Khyathisree, Prasanthi Boyapati, LV Siva Rama Krishna Boddu, and Saibaba Velidi. "Used Car Price Forecasting: A Machine Learning-Based Approach." In Algorithms in Advanced Artificial Intelligence, pp. 465-470. CRC Press, 2025.
[20] Krishna, Boddu & Mahalakshmi, V. & Gopala Krishna Murthy, Nookala. (2023). Modelling a stacked dense network model for outlier prediction over medical-based heart prediction data. Journal of High Speed Networks. 29. 1-16. 10.3233/JHS-222079.
[21] M. V. Babu, V. Ramya, and V. S. Murugan, "Implementation of wearable device for upper limb rehabilitation using embedded IoT," Int. J. Electron. Signals Syst. Manag. Sci., vol. 16, no. 1, pp. 90–95, Mar. 2024. [Online]. Available: https://doi.org/10.1504/IJESMS.2024.136972
[22] M. V. . Babu, V. . Ramya, and V. S. . Murugan, "A Proposed High Efficient Current Control Technique for Home Based Upper Limb Rehabilitation and Health Monitoring System during Post Covid-19", Int J Intell Syst Appl Eng, vol. 12, no. 2s, pp. 600–607, Oct. 2023.
[23] Mr Sasidhar Reddy Gaddam and DOI : 10.48047/IJCNIS.14.3.1283, "Java-Driven Trustworthy And Reliable Deep Learning For Cyberattack Detection In Industrial Iot", Int. j. commun. netw. inf. secur., vol. 14, no. 3, pp. 1274–1283, Apr. 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY