International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

An Intelligent Machine Learning Framework for Cyber Attack Detection in Secure UAV Communication Networks

Miss. Kathula Lakshmi[1], Miss. Savarapu Suhasini[2]
MTech in department of computer Science and Engineering, 2 HOD of Computer science and Engineering In Lenora college of engineering, rampachodavaram , alluri seetharama raju district , Andhra Pradesh, India

Abstract — The rapid adoption of Unmanned Aerial Vehicles (UAVs) in applications such as surveillance, precision agriculture, disaster response, logistics, and intelligent transportation has significantly increased the demand for secure and reliable communication networks. However, the wireless nature of UAV communication exposes these systems to a wide range of cyber threats, including GPS spoofing, data injection, denial-of-service (DoS), and network intrusion attacks, which can compromise mission integrity and operational safety. To address these security challenges, this paper presents a machine learning-based cyber attack detection framework for UAV communication networks. The proposed framework employs comprehensive data preprocessing, feature engineering, and intelligent classification techniques to analyze UAV telemetry data, communication signals, and operational parameters for identifying malicious activities. Multiple machine learning models are utilized to distinguish normal UAV behavior from cyber attack scenarios through behavioral pattern analysis and anomaly detection. The framework is evaluated using standard performance metrics, including accuracy, precision, recall, F1-score, and ROC-AUC, to assess its detection capability and reliability. Experimental results demonstrate that the proposed framework effectively detects various cyber attacks with high detection accuracy, low false positive rates, and efficient response time. By integrating intelligent machine learning algorithms into UAV cybersecurity, the proposed approach enhances communication security, improves system resilience, and supports the development of reliable and autonomous drone operations in dynamic network environments.

Keywords— Unmanned Aerial Vehicles (UAVs), Drone Cybersecurity, Machine Learning, Intrusion Detection, Anomaly Detection, UAV Communication Networks, GPS Spoofing, Network Security, Cyber Attack Detection.

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have emerged as a transformative technology across numerous civilian and military applications. Their ability to operate autonomously, collect real-time information, and perform complex missions with minimal human intervention has made UAVs indispensable in areas such as surveillance, precision agriculture, environmental monitoring, disaster response, logistics, border security, and smart city management [2], [9]. As UAV technology continues to evolve, modern drone systems increasingly rely on wireless communication networks to exchange mission-critical information with ground control stations, onboard sensors, cloud platforms, and other connected devices.

Despite their operational advantages, UAV communication networks remain highly susceptible to cyber threats due to their open and distributed communication architecture. Sensitive information, including telemetry data, navigation commands, sensor measurements, and control signals, is continuously transmitted through wireless channels that can be exploited by malicious attackers. Cyber attacks targeting UAV systems can disrupt communication, manipulate navigation data, compromise mission objectives, and threaten both operational safety and data confidentiality [1], [9].

Several forms of cyber attacks have been reported in UAV environments, including GPS spoofing, false data injection, denial-of-service (DoS), communication jamming, and unauthorized network intrusion. These attacks may alter UAV flight trajectories, interrupt communication links, inject malicious commands, or gain unauthorized control over drone operations. Such security breaches can result in mission failure, information leakage, equipment damage, and significant safety risks, particularly in critical applications such as defense, emergency response, and infrastructure monitoring [4], [6], [11].

Conventional cybersecurity solutions, including signature-based intrusion detection systems and rule-based security mechanisms, are often ineffective against sophisticated and previously unseen cyber attacks. These traditional approaches primarily depend on predefined attack signatures and static security rules, limiting their ability to identify evolving attack

patterns and zero-day threats. Consequently, there is a growing demand for intelligent cybersecurity frameworks capable of adapting to dynamic threat environments while maintaining high detection accuracy and low false alarm rates [10], [14].
Recent advances in machine learning have provided promising solutions for strengthening UAV cybersecurity. Machine learning algorithms can automatically analyze large volumes of telemetry data, communication signals, and operational parameters to learn normal system behavior and identify abnormal activities that indicate potential cyber attacks. Supervised learning, anomaly detection techniques, and neural network-based intrusion detection systems have demonstrated significant potential in detecting both known and previously unknown attacks while supporting real-time threat identification and response [12], [13], [16].

Motivated by these advancements, this research proposes a machine learning-based cyber attack detection framework for secure UAV communication networks. The proposed framework combines data preprocessing, feature engineering, machine learning-based classification, anomaly detection, and real-time monitoring to identify malicious activities affecting UAV operations. By leveraging intelligent learning techniques, the framework enhances cyber threat detection capability, improves communication security, and increases the overall reliability and resilience of UAV communication systems operating in dynamic and hostile environments.

The remainder of this paper is organized as follows. Section II reviews recent research related to UAV cybersecurity and machine learning-based intrusion detection techniques. Section III presents the system analysis and proposed methodology. Section IV describes the system architecture and design. Section V discusses the implementation modules, while Section VI presents the experimental results and performance evaluation. Finally, Section VII concludes the paper and outlines future research directions.

II. LITERATURE SURVEY

The rapid expansion of Unmanned Aerial Vehicle (UAV) applications has significantly increased the need for secure communication infrastructures capable of protecting drones from evolving cyber threats. Since UAVs rely extensively on wireless communication for navigation, telemetry exchange, and mission execution, they are exposed to various cybersecurity risks. Consequently, researchers have proposed several security mechanisms, including intrusion detection systems, anomaly detection models, blockchain-based frameworks, and machine learning techniques to enhance the resilience of UAV communication networks [1], [2].

Early research on UAV cybersecurity primarily focused on identifying vulnerabilities within wireless communication protocols and control systems. Conventional security solutions such as encryption methods, authentication protocols, and rule-based intrusion detection systems were developed to safeguard communication channels from unauthorized access. Although these approaches provide basic protection against known attacks, they often struggle to detect sophisticated and previously unseen cyber threats due to their dependence on predefined attack signatures [5], [6].

With the increasing complexity of cyber attacks, researchers have explored intelligent anomaly detection techniques capable of identifying abnormal UAV behavior. Several studies have demonstrated that monitoring changes in telemetry data, navigation parameters, communication latency, and sensor measurements enables early detection of attacks such as GPS spoofing, data injection, communication jamming, and denial-of-service (DoS). These behavioral analysis techniques significantly improve the reliability of UAV security systems by identifying deviations from normal operational patterns [4], [7], [9].

Recent advancements in machine learning have transformed UAV cybersecurity by enabling automated detection of malicious activities through data-driven analysis. Supervised learning algorithms, including Random Forest, Support Vector Machine (SVM), Artificial Neural Networks (ANN), and other ensemble learning techniques, have shown excellent performance in classifying normal and malicious UAV operations. These intelligent models learn complex behavioral patterns from historical telemetry data, allowing them to detect both known and unknown cyber attacks with improved accuracy and lower false alarm rates [10]–[13].

Researchers have also investigated advanced security frameworks that combine machine learning with emerging technologies such as blockchain, Internet of Things (IoT), and deep learning. Blockchain-based architectures improve communication integrity through decentralized authentication, while deep learning models enhance intrusion detection by learning complex feature representations from large UAV datasets. Hybrid security frameworks integrating multiple intelligent technologies have demonstrated promising improvements in detection accuracy, scalability, and real-time threat response for autonomous drone networks [3], [15], [16], [19].

Although considerable progress has been achieved in securing UAV communication networks, several challenges remain. Existing detection systems often experience limitations in

computational efficiency, adaptability to zero-day attacks, real-time response capability, and deployment on resource-constrained UAV platforms. Therefore, developing lightweight and intelligent machine learning frameworks capable of accurately detecting multiple cyber-attack scenarios while maintaining low computational overhead continues to be an important research direction. Such frameworks are expected to improve the reliability, security, and operational resilience of next-generation UAV communication networks operating in dynamic environments [11], [16], [18], [20].

III. SYSTEM ANALYSIS

1. Existing System

Existing cybersecurity solutions for Unmanned Aerial Vehicle (UAV) communication networks primarily rely on conventional intrusion detection systems, rule-based security mechanisms, encryption techniques, and authentication protocols to safeguard drone operations. These methods monitor communication traffic, telemetry information, and control signals to identify suspicious activities and prevent unauthorized access to UAV systems. Signature-based intrusion detection systems are widely used to recognize previously known attack patterns by comparing network behavior against predefined attack signatures and security rules [5], [6].

In recent years, several machine learning approaches have also been introduced to improve UAV cybersecurity. Algorithms such as Support Vector Machine (SVM), Artificial Neural Networks (ANN), and Decision Tree-based classifiers have been employed to analyze telemetry data, navigation parameters, and communication signals for detecting cyber attacks. These approaches have shown promising results in identifying attacks such as GPS spoofing, data injection, denial-of-service (DoS), and network intrusion attempts by learning behavioral patterns from historical UAV operational data [8], [10], [13].

Although these techniques improve cyber threat detection, existing frameworks still face significant limitations when deployed in real-world UAV environments. Many security models are designed to detect only specific attack categories and often struggle to recognize previously unseen or rapidly evolving cyber threats. Furthermore, variations in communication patterns, dynamic flight conditions, and resource limitations of UAV platforms reduce the overall effectiveness of existing detection systems. Consequently, achieving accurate, real-time, and adaptive cyber attack detection remains a major challenge in securing UAV communication networks [1], [9], [16].

Disadvantages of the Existing System

- Limited Detection Capability: Conventional intrusion detection systems primarily rely on predefined attack signatures, making them ineffective against zero-day attacks and newly emerging cyber threats [5], [10].
- Low Adaptability: Existing security frameworks often fail to adapt to evolving attack strategies and dynamic communication environments commonly observed in UAV networks [1], [16].
- High False Alarm Rate: Many traditional detection methods generate false positives when distinguishing between legitimate UAV operational variations and malicious activities, reducing overall system reliability [8], [13].
- Computational Constraints: Advanced security algorithms may require considerable computational resources and memory, making them difficult to deploy on lightweight UAV platforms with limited processing capabilities [3], [15].
- Poor Real-Time Performance: Some existing approaches experience delays in processing telemetry data and communication signals, limiting their effectiveness in detecting and responding to cyber-attacks during active UAV missions [4], [11].
- Limited Generalization: Models trained using specific datasets often perform poorly when exposed to new operational environments, communication protocols, or previously unseen attack scenarios, resulting in reduced detection accuracy [10], [16].
- Scalability Challenges: As UAV communication networks continue to expand with multiple drones, IoT devices, and cloud-based services, many existing cybersecurity frameworks struggle to maintain consistent detection performance and efficient resource utilization [2], [19].

2. Proposed System

The proposed system presents an intelligent machine learning-based cyber attack detection framework designed to enhance the security of Unmanned Aerial Vehicle (UAV) communication networks. The framework combines data preprocessing, feature engineering, supervised machine learning, anomaly detection, and real-time monitoring to accurately identify malicious activities affecting UAV operations. By integrating intelligent learning techniques with behavioral analysis, the proposed framework improves attack detection capability while maintaining reliable system performance under dynamic network conditions [10], [13], [16].

Initially, UAV operational data is collected from telemetry logs, communication channels, navigation systems, and onboard sensors. The collected dataset undergoes a comprehensive preprocessing stage that includes noise removal, missing value handling, feature normalization, and data cleaning. These preprocessing operations improve data quality, eliminate inconsistencies, and ensure that the machine learning models receive reliable input for accurate cyber attack detection [8], [11].

Following preprocessing, feature engineering techniques are employed to identify the most informative UAV operational parameters. Critical features such as GPS coordinates, flight altitude, communication latency, navigation commands, sensor measurements, signal strength, battery status, and network traffic patterns are extracted and analysed. Dimensionality reduction methods, including Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), are incorporated to reduce computational complexity while preserving the most significant information required for classification [7], [12].

The optimized feature set is then utilized to train multiple machine learning models, including Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN). These algorithms learn the behavioral characteristics of normal UAV operations and distinguish them from malicious activities such as GPS spoofing, false data injection, denial-of-service attacks, and unauthorized network access. The combination of multiple classification models enhances detection accuracy and improves the framework's adaptability to evolving cyber threats [10], [13], [18].

To strengthen security against previously unseen attacks, the proposed framework incorporates anomaly detection techniques alongside supervised learning models. Intelligent anomaly detection continuously monitors UAV telemetry data and communication behavior to identify abnormal operational patterns that may indicate zero-day attacks or unknown security threats. This hybrid detection strategy significantly improves the robustness and reliability of the cybersecurity framework by enabling early identification of malicious activities before they compromise UAV operations [4], [15], [16].

The proposed framework further integrates a real-time monitoring and alert generation mechanism that continuously analyzes incoming UAV communication data during flight operations. Whenever suspicious behavior is detected, the system generates immediate security alerts, enabling rapid response and mitigation of potential cyber attacks. The performance of the framework is evaluated using standard metrics such as accuracy, precision, recall, F1-score, and ROC-AUC to validate its effectiveness in detecting diverse cyber attack scenarios [11], [16], [20].

Overall, the proposed machine learning-based framework provides a scalable, intelligent, and computationally efficient solution for securing UAV communication networks. By combining advanced machine learning algorithms with continuous behavioral monitoring, the framework enhances cyber threat detection, improves operational resilience, and supports the secure deployment of autonomous UAV systems across critical real-world applications such as surveillance, disaster management, smart transportation, and defense operations [1], [10], [19].

IV. SYSTEM DESIGN

1. System Architecture

Below diagram depicts the whole system architecture.

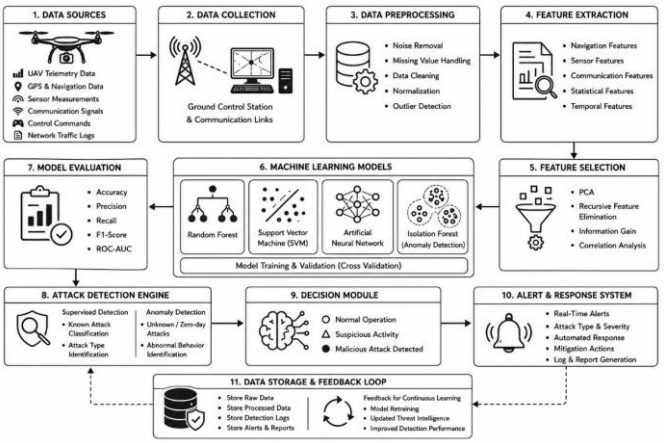

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

1. Modules

UAV Data Acquisition and Preprocessing Module

This module is responsible for collecting UAV operational data from telemetry systems, onboard sensors, communication channels, and ground control stations. The collected dataset includes parameters such as GPS coordinates, altitude, velocity, battery status, communication latency, navigation commands, signal strength, and network traffic information. Before analysis, the data undergoes preprocessing operations including noise removal, missing value imputation, normalization, and outlier elimination. These preprocessing techniques improve data quality, ensure consistency, and enhance the performance

of the machine learning models used for cyber attack detection [8], [11].

Feature Engineering and Selection Module
After preprocessing, the system extracts meaningful features that accurately represent UAV operational behavior. Important attributes such as navigation patterns, communication signals, sensor measurements, control commands, and network activity are analyzed to distinguish normal operations from malicious behavior. Feature selection techniques, including Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), are applied to reduce dimensionality by retaining only the most informative features. This process minimizes computational complexity while improving detection accuracy and model efficiency [7], [12].

Machine Learning Model Development Module
The optimized feature set is utilized to train multiple machine learning classifiers capable of identifying cyber attacks affecting UAV communication networks. Algorithms such as Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN) are trained using labelled datasets containing both normal UAV operations and various attack scenarios. These models learn complex behavioral patterns and establish decision boundaries that enable accurate classification of legitimate and malicious activities. Comparative evaluation is performed to identify the most effective model for cyber attack detection [10], [11], [13].

Intelligent Anomaly Detection Module
To improve security against emerging cyber threats, the proposed framework incorporates an intelligent anomaly detection module. In addition to supervised classification, anomaly detection algorithms continuously monitor UAV telemetry data and communication behavior to identify deviations from normal operational patterns. This module enables the detection of previously unseen attacks such as zero-day exploits, GPS spoofing, false data injection, denial-of-service attacks, and unauthorized network intrusions. The integration of supervised learning and anomaly detection significantly enhances the robustness and adaptability of the proposed cybersecurity framework [4], [15], [16].

Real-Time Monitoring and Alert Generation Module
The final module continuously monitors incoming UAV communication data during flight operations. The trained machine learning models analyze telemetry streams in real time to detect suspicious activities and classify potential cyber threats. Whenever abnormal behavior is identified, the system immediately generates security alerts and notifies the ground control station for timely mitigation. The framework also logs detected events for future analysis and system improvement. Real-time monitoring enables rapid threat response, improves mission reliability, and enhances the overall resilience of UAV communication networks operating in dynamic environments [11], [16], [20].

VI. RESULTS AND DISCUSSION

This section presents the experimental evaluation of the proposed machine learning-based cybersecurity framework developed for securing UAV communication networks. The experiments were performed using UAV telemetry datasets containing both normal flight operations and multiple simulated cyber attack scenarios. The collected telemetry information, communication signals, navigation parameters, and system performance metrics were pre-processed and used to train different machine learning models. The effectiveness of the proposed framework was evaluated by comparing classification performance, analyzing attack detection capability, and assessing the model's ability to distinguish malicious UAV behavior from legitimate operations [10], [13].

A. Performance Comparison of Machine Learning Models
To identify the most suitable classification algorithm for UAV cyber attack detection, three machine learning models were implemented and evaluated: Support Vector Machine (SVM), Artificial Neural Network (ANN), and Random Forest. Each model was trained using historical UAV telemetry data consisting of both normal operational behavior and cyber attack samples, including GPS spoofing, false data injection, and network intrusion attacks. Model performance was evaluated using common classification metrics such as accuracy, precision, recall, and F1-score.

Table 1. Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score
Support Vector Machine	90.2	0.89	0.88	0.88
Artificial Neural Network	92.8	0.91	0.90	0.90
Random Forest	95.1	0.94	0.93	0.93

The experimental results demonstrate that the Random Forest classifier achieved the highest overall performance, obtaining a classification accuracy of 95.1%. Its ensemble learning strategy effectively combines multiple decision trees, improving

classification stability, minimizing overfitting, and enhancing the detection of diverse cyber attack patterns compared to the other evaluated models [10], [11].

2. ROC Curve Analysis

Receiver Operating Characteristic (ROC) analysis was conducted to evaluate the classification capability of the proposed cyber attack detection framework under different decision thresholds. The ROC curve illustrates the relationship between the True Positive Rate (TPR) and the False Positive Rate (FPR), providing a comprehensive measure of the classifier's discrimination capability.

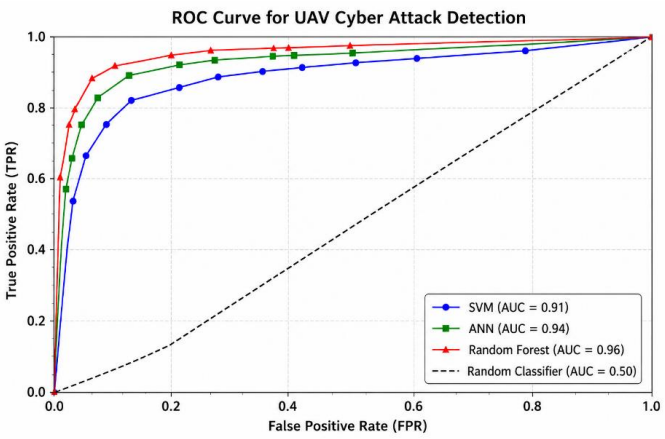

Fig. 2. ROC Curve for UAV Cyber Attack Detection Model

The Random Forest classifier achieved an Area Under the Curve (AUC) value of approximately 0.96, indicating excellent classification performance and a strong ability to differentiate malicious UAV activities from normal operational behavior. The high ROC-AUC score confirms that the proposed framework maintains reliable detection performance even under complex communication conditions and diverse cyber attack scenarios [11], [13].

3. Confusion Matrix Analysis

To further evaluate classification performance, a confusion matrix was generated to compare the predicted attack classes with the actual UAV operational labels.

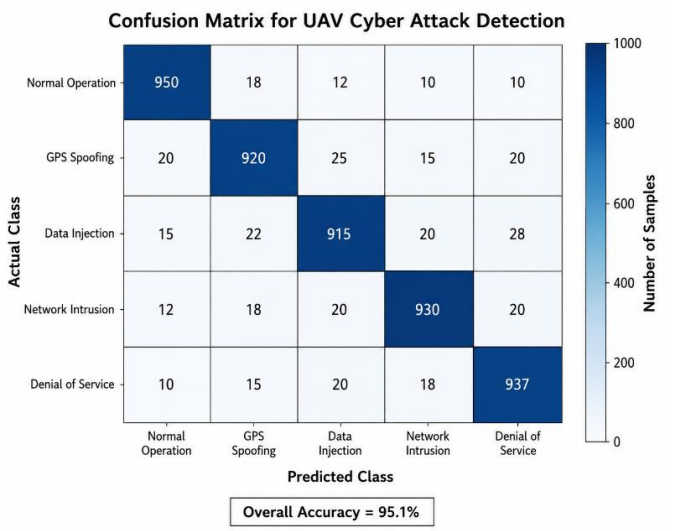

Fig. 3. Confusion Matrix for UAV Cyber Attack Detection

The confusion matrix indicates that the majority of normal operations and cyber attack instances were correctly classified by the proposed model, with only a small number of misclassified samples. Most predictions are concentrated along the principal diagonal of the matrix, demonstrating high classification accuracy and reliable attack identification. The results confirm that the framework effectively detects multiple cyber threats, including GPS spoofing, false data injection, and network intrusion attempts while maintaining a low false positive rate [8], [11].

The confusion matrix also provides valuable insight into model behavior by identifying attack categories that are occasionally misclassified. Such analysis supports further optimization of feature engineering and model tuning, ultimately improving detection accuracy and strengthening the cybersecurity of UAV communication networks.

VII. CONCLUSION AND FUTURE WORK

This paper presented an intelligent machine learning-based cyber attack detection framework for enhancing the security of Unmanned Aerial Vehicle (UAV) communication networks. The proposed framework utilizes UAV telemetry data, communication signals, navigation parameters, and operational information to accurately distinguish normal system behavior from malicious activities. A systematic pipeline comprising data preprocessing, feature engineering, machine learning-based classification, anomaly detection, and real-time monitoring was developed to improve the effectiveness of cyber threat detection in UAV environments [10], [13], [16].

Experimental evaluation demonstrated that the proposed framework effectively detects multiple cyber attack scenarios, including GPS spoofing, false data injection, network intrusion, and denial-of-service attacks. Among the evaluated machine learning algorithms, the Random Forest classifier achieved the highest detection performance, providing superior accuracy, precision, recall, and F1-score while maintaining a low false positive rate. The integration of intelligent feature selection and anomaly detection further improved the robustness, reliability, and adaptability of the framework, making it suitable for deployment in dynamic UAV communication networks [8], [10], [11].

The proposed framework offers a scalable and computationally efficient solution for strengthening UAV cybersecurity and supporting secure autonomous drone operations across applications such as surveillance, disaster management, environmental monitoring, military missions, and smart city infrastructure. By enabling early detection of malicious activities, the framework enhances communication reliability, operational safety, and overall network resilience [1], [9], [19]. Future research can focus on integrating advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks, Graph Neural Networks (GNNs), Vision Transformers (ViTs), and federated learning techniques to improve the detection of complex and evolving cyber threats. The incorporation of Explainable Artificial Intelligence (XAI) can further enhance the transparency and interpretability of machine learning decisions. In addition, integrating blockchain-based authentication, edge computing, and Internet of Things (IoT)-enabled security mechanisms can strengthen communication integrity while reducing response latency. Evaluating the proposed framework using large-scale real-world UAV datasets and deploying it in operational drone environments will further validate its effectiveness and contribute to the development of secure, intelligent, and resilient next-generation UAV communication systems [3], [15], [16], [20].

REFERENCES

1. A. E. Omolara, M. Alawida, and O. I. Abiodun, “Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey,” Neural Computing and Applications, vol. 35, no. 31, pp. 23063–23101, 2023.
2. E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya, and S. Uluağaç, “Drones for smart cities: Issues in cybersecurity, privacy, and public safety,” in Proc. IEEE Int. Wireless Communications and Mobile Computing Conference (IWCMC), Sep. 2016, pp. 216–221.
3. A. Ossamah, “Blockchain as a solution to drone cybersecurity,” in Proc. IEEE 6th World Forum on Internet of Things (WF-IoT), Jun. 2020, pp. 1–9.
4. J. Xiao and M. Feroskhan, “Cyber attack detection and isolation for a quadrotor UAV with modified sliding innovation sequences,” IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 7202–7214, 2022.
5. H. Sedjelmaci, S. M. Senouci, and N. Ansari, “A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1594–1606, 2017.
6. H. Sedjelmaci, S. M. Senouci, and M. A. Messous, “How to detect cyber-attacks in unmanned aerial vehicles network?” in Proc. IEEE Global Communications Conference (GLOBECOM), Dec. 2016, pp. 1–6.
7. E. Basan, A. Basan, A. Nekrasov, C. Fidge, J. Gamec, and M. Gamcová, “A self-diagnosis method for detecting UAV cyber attacks based on analysis of parameter changes,” Sensors, vol. 21, no. 2, p. 509, 2021.
8. A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, “Detection of fault data injection attack on UAV using adaptive neural network,” Procedia Computer Science, vol. 95, pp. 193–200, 2016.
9. M. R. Manesh and N. Kaabouch, “Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,” Computers & Security, vol. 85, pp. 386–401, 2019.
10. A. Handa, A. Sharma, and S. K. Shukla, “Machine learning in cybersecurity: A review,” Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 9, no. 4, p. e1306, 2019.
11. Z. Baig, N. Syed, and N. Mohammad, “Securing the smart city airspace: Drone cyber attack detection through machine learning,” Future Internet, vol. 14, no. 7, p. 205, 2022.
12. N. Moustafa and A. Jolfaei, “Autonomous detection of malicious events using machine learning models in drone networks,” in Proc. ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, Sep. 2020, pp. 61–66.
13. R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, “Machine-learning-enabled intrusion detection system for cellular connected UAV networks,” Electronics, vol. 10, no. 13, p. 1549, 2021.
14. S. Ouiazzane, M. Addou, and F. Barramou, “A multiagent and machine learning based denial of service intrusion detection system for drone networks,” in Geospatial Intelligence: Applications and Future Trends, pp. 51–65, 2022.

15. M. Y. Alzahrani, "Enhancing drone security through multi-sensor anomaly detection and machine learning," SN Computer Science, vol. 5, no. 5, p. 651, 2024.
16. A. Aldaej, T. A. Ahanger, M. Atiquzzaman, I. Ullah, and M. Yousufudin, "Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective," Sensors, vol. 22, no. 7, p. 2630, 2022.
17. R. A. Ramadan, A. H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," Electronics, vol. 10, no. 21, p. 2633, 2021.
18. D. S. Prasad, P. Jyothi, G. Suryanarayana, and S. N. Mohanty, "Algorithms to mitigate cybersecurity threats by employing intelligent machine learning models in the design of IoT-aided drones," in Drone Technology: Future Trends and Practical Applications, pp. 257–300, 2023.
19. S. N. Ashraf et al., "IoT empowered smart cybersecurity framework for intrusion detection in internet of drones," Scientific Reports, vol. 13, no. 1, p. 18422, 2023.
20. A. Al-Fuwaiers and S. Mishra, "ML-based intrusion detection for drone IoT security," Journal of Cybersecurity & Information Management, vol. 14, no. 1, 2024.

AUTHOR DETAIL

Miss. Kathula Lakshmi is currently pursuing M.Tech in Computer Science and Engineering at Lenora College of Engineering, Rampachodavaram, Alluri Sitarama Raju District, Andhra Pradesh, India. She possesses a strong academic foundation in Machine Learning, Cybersecurity, Computer Networks, Java Programming, Web Technologies, and Database Management Systems. Her practical experience includes developing intelligent cyber defence systems involving data preprocessing, feature engineering, model training, attack detection, and performance evaluation using machine learning techniques. Her work focuses on implementing intelligent predictive models for cyber-attack detection in secure Unmanned Aerial Vehicle (UAV) communication networks, enhancing the security, reliability, and resilience of next-generation wireless communication systems. She is also experienced in software system design using Unified Modelling Language (UML), including use case, class, sequence, activity, and data flow diagrams. Her research interests include Machine Learning, Cybersecurity, UAV Communication Networks, Intrusion Detection Systems, Network Security, and Intelligent Threat Detection. She is committed to advancing academic research and developing innovative AI-driven solutions for secure communication systems and intelligent cyber defence technologies.

Miss. SAVARAPU SUHASINI is the Head of the Department of Computer Science and Engineering at Lenora College of Engineering, Rampachodavaram, Alluri Sitarama Raju District, Andhra Pradesh, India. She possesses extensive academic and research expertise in Machine Learning, Artificial Intelligence, Natural Language Processing (NLP), Data Science, Computer Vision, Web Technologies, and Database Management Systems. She has guided numerous postgraduate research projects in emerging domains of intelligent computing, with a strong emphasis on the design, development, and evaluation of AI-driven solutions for real-world applications. Her research interests encompass Machine Learning, Deep Learning, Natural Language Processing, Explainable Artificial Intelligence (XAI), Intelligent Data Analytics, Computer Vision, and Predictive Modelling. She has significant experience in software engineering methodologies, system analysis, and Unified Modelling Language (UML)-based software design, including use case, class, sequence, activity, and data flow diagrams. As an academic mentor and researcher, she is committed to promoting excellence in teaching, fostering innovative research, and developing intelligent computational frameworks that address contemporary challenges in artificial intelligence and data-driven technologies.