International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Research

AI Based Intrusion Detection for Drones

Mr.Potharapu Sravan Kumar, Assistant Professor, Dept of CSE(AI&ML), Sreenidhi Institute of Science and Technology Hyderabad, India, sravankumar777@gmail.com

Pollampally Bhuvaneshwar, Department of CSE(AI&ML), Sreenidhi Institute of Science and Technology Hyderabad, India, Bhuvaneshwarpollampally@gmail.com
Guttikonda Nandan, Department of CSE(AI&ML), Sreenidhi Institute of Science and Technology Hyderabad, India, nandanguttikonda2004@gmail.com
Pothula Koushik Reddy, Department of CSE(AI&ML), Sreenidhi Institute of Science and Technology Hyderabad, India, pothulakoushik09@gmail.com

***Abstract*—Drones are being used more and more in things like watching over places delivering packages checking on disasters and sensing things from away. This means that the amount of information being sent over networks by drones is getting really big. These drone networks need to be able to talk to each other all the time so they can work with ground control stations and cloud servers.**

This also makes them more open to cyber threats like fake messages extra information being added and people getting in without permission. So, we need safe ways to watch over the traffic on these drone networks. This research is about making a system that uses intelligence to detect when someone is trying to get into the drone network.

The system uses a different way to figure out what is going on with the network traffic, including Random Forest Classifier, Gradient Boosting Classifier, Decision Tree and Support Vector Machine. It looks at things like how traffic there is, how different the packet sizes are and what kind of internet control messages are being sent.

The system tries to guess what kind of request is being made over the internet and sorts the network traffic to find anything that might be a problem. By learning what the network usually does the system can find things that're not normal and might mean someone is trying to get in without permission.

When we tested the system, we found that the Random Forest and Gradient Boosting classifiers were really good at guessing what was going on and stayed stable when the network was changing.

The results showed that using intelligence to detect problems with the drone network made it more secure and worked better.

The system helps reduce delays loses information finds bad traffic early and makes sure that information is sent reliably between drones and the control systems. Also using machine learning with drone networks means that the security can adapt to threats.

Overall, this way of doing things makes drone networks more able to deal with problems keeps the information safe and can find threats in time which is good, for modern drone applications that work in complicated and busy network environments. Drone networks and drones are important here. We need to make sure drones and drone networks are safe and secure.

Keywords: Drone Network Security, Intrusion Detection System (IDS), Machine Learning, Unmanned Aerial Vehicles (UAV), Network Traffic Analysis, Cybersecurity for Drone Networks

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have rapidly evolved into essential components of modern technological ecosystems. They are widely used in various applications such as surveillance, disaster management, environmental monitoring, package delivery, agriculture, and military operations. The ability of drones to collect and transmit real-time data through wireless communication networks has significantly improved operational efficiency in many domains. However, the increasing reliance on drone networks has also introduced serious cybersecurity challenges, as these systems are highly vulnerable to cyber-attacks, unauthorized access, data interception, and network intrusions.

Drone communication systems typically rely on continuous interaction between UAVs, ground control stations, cloud platforms, and edge devices. These communications generate large volumes of network traffic that must be monitored and secured in real time. Traditional security mechanisms, such as rule-based intrusion detection systems and signature-based methods, are often insufficient for drone networks because they struggle to detect unknown or evolving cyber threats. Attackers can exploit vulnerabilities in wireless communication protocols to launch spoofing, denial-of-service (DoS), man-in-the-middle, packet-injection, and unauthorized command-execution attacks. These threats can compromise drone operations, disrupt mission-critical tasks, and potentially lead to severe safety risks.

To address these challenges, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for enhancing cybersecurity in drone networks. AI-based intrusion detection systems can automatically analyses large volumes of network traffic data and identify abnormal patterns

that indicate potential attacks. Unlike traditional methods, machine learning algorithms can learn from historical network behavior and adapt to new attack patterns, thereby enabling more accurate and efficient detection of malicious activity.

In recent years, several machine learning approaches have been applied to intrusion detection in UAV networks. Algorithms such as Random Forest, Support Vector Machine (SVM), Decision Tree, Gradient Boosting, and Neural Networks have demonstrated strong capabilities in analyzing network traffic features and detecting anomalies. These models can process various traffic parameters, including traffic volume, packet size variance, TCP window size, ICMP type, and other network characteristics, to classify normal and malicious network activities. By identifying irregular communication patterns, machine learning models can detect intrusions at an early stage and prevent potential security breaches.

Motivated by these advancements, this research proposes an AI-based intrusion detection framework for drone communication networks. The proposed system utilises multiple machine learning models, including Random Forest Classifier (RFC), Gradient Boosting Classifier (GBC), Decision Tree (DT), and Support Vector Machine (SVM), to analyses drone network traffic and classify HTTP request methods for improved intrusion detection. The framework leverages network traffic features to identify abnormal communication patterns between drones and control servers.

The main objective of this study is to develop an intelligent security mechanism capable of detecting network intrusions, improving communication reliability, and optimizing traffic management in drone networks. By applying machine learning techniques, the proposed system aims to enhance drone communication security, reduce network delays, minimize packet loss, and improve the overall performance of UAV networks.

The remainder of this paper is organized as follows: Section II presents the literature review on AI-based intrusion detection and drone network security. Section III describes the proposed methodology and machine learning framework. Section IV discusses the experimental results and performance evaluation. Finally, Section V concludes the paper and outlines future research directions for improving drone network security.

II. LITERATURE SURVEY

With the rapid development of Unmanned Aerial Vehicles (UAVs) and their increasing deployment in applications such as surveillance, disaster response, agriculture monitoring, and logistics delivery, ensuring secure communication within drone networks has become a major research challenge. Drone networks rely heavily on wireless communication between UAVs, ground control stations, and cloud infrastructures. Due to this dependency, UAV systems are highly vulnerable to cyber threats, including spoofing attacks, jamming, denial-of-service (DoS), and unauthorized control commands. To address these issues, several researchers have explored Artificial Intelligence (AI) and Machine Learning (ML) based intrusion detection systems (IDS) for securing drone communication networks.

1. Machine Learning-Based Intrusion Detection for UAV Networks Sharma et al. proposed a machine learning-based intrusion detection system using Support Vector Machine (SVM) and Decision Tree algorithms to analyse UAV communication traffic. Their study demonstrated that ML-based models could effectively detect abnormal network patterns compared to traditional rule-based intrusion detection methods. However, the system required large training datasets and struggled with highly dynamic network environments.

2. Deep Learning Approach for UAV Network Security Khan et al. introduced a deep learning-based security framework for drone networks using Artificial Neural Networks (ANN) and Convolutional Neural Networks (CNN). The proposed system was capable of detecting cyber attacks such as spoofing, jamming, and denial-of-service attacks. Although the model achieved high detection accuracy, its computational complexity made it difficult to implement on lightweight UAV hardware systems.

3. Random Forest-Based Intrusion Detection for UAV Communication Gupta and Patel developed an intrusion detection model using the Random Forest algorithm to analyses UAV communication traffic. The model used features such as packet transmission rate, network latency, and packet size to classify normal and malicious activities. The results showed that Random Forest provided better accuracy and robustness compared to several traditional machine learning algorithms.

4. Hybrid Machine Learning Model for UAV Cybersecurity Li et al. proposed a hybrid intrusion detection model that combined Support Vector Machine and Gradient Boosting techniques to enhance detection performance in UAV networks. The hybrid model improved classification accuracy and detection efficiency. However, combining multiple models increased the computational overhead and reduced the feasibility of real-time deployment.

5. Network Traffic Analysis for Drone Security Zhang et al. conducted a study focusing on network traffic behavior analysis in UAV communication systems. The research examined traffic features such as TCP window size, packet variance, and request types to detect abnormal communication patterns. While the system successfully identified anomalies, it lacked adaptive learning capabilities to detect new attack patterns.

6. AI-Based Cybersecurity Framework for UAV Systems Recent studies have proposed AI-driven frameworks for securing UAV networks through real-time anomaly detection and automated traffic monitoring. These frameworks integrate machine learning models with drone communication protocols to detect malicious traffic in real time. Although such systems improve network security, they still face challenges related to scalability, computational efficiency, and handling large-scale UAV networks.

7. Intrusion Detection Using Gradient Boosting for UAV Networks Ahmed et al. proposed an intrusion detection system using Gradient Boosting classifiers for analysing drone communication traffic. Their approach achieved higher classification accuracy by learning complex patterns from network traffic data. However, the training process required high computational resources and extensive feature engineering.

8. UAV Security Using Ensemble Learning Models Singh et al. investigated the use of ensemble learning methods, including Random Forest and Gradient Boosting algorithms, to improve the reliability of intrusion detection systems for UAV networks. The ensemble approach improved detection accuracy and reduced false positives. However, the model complexity increased the system processing time.

9. Intelligent Drone Network Monitoring Using Machine Learning Recent research has explored intelligent monitoring systems that use machine learning algorithms to analyse communication traffic between UAVs and ground stations. These systems focus on detecting abnormal patterns in network parameters such as traffic volume, latency, and packet loss. The results indicate that machine learning models can significantly improve the reliability and security of UAV communication networks.

Research Gap

From the existing literature, it is evident that AI-based intrusion detection systems have significantly improved cybersecurity in drone networks. However, many current approaches face limitations such as high computational complexity, insufficient real-time detection capability, and limited evaluation of multiple machine learning algorithms. Additionally, some studies focus on individual models without comparing their performance in dynamic network environments.

To address these limitations, this research proposes an AI-based intrusion detection framework that evaluates multiple machine learning models—including Random Forest Classifier, Gradient Boosting Classifier, Decision Tree, and Support Vector Machine—to improve intrusion detection accuracy and network efficiency in drone communication systems. The proposed framework aims to provide a more robust and efficient security solution for modern UAV networks.

III. ALGORITHM

The proposed system utilises Artificial Intelligence and Machine Learning techniques to detect intrusions in drone communication networks. The algorithm analyses network traffic data generated between drones and ground control stations to identify abnormal patterns that may indicate cyber-attacks, such as spoofing, packet injection, or denial-of-service attacks.

The system evaluates four machine learning models:

- Random Forest Classifier (RFC)
- Gradient Boosting Classifier (GBC)
- Decision Tree (DT)
- Support Vector Machine (SVM)

These models classify network requests and detect suspicious traffic behaviour in real time.

Input: Network traffic dataset D containing features such as traffic_volume, packet_size_variance, tcp_window_size, icmp_type, http_method, and request_frequency.

Output: Classification of network traffic as Normal or Malicious.

Step 1: Data Collection: Network traffic data is collected from UAV communication systems. Packets exchanged between drones, ground control stations, and cloud servers are captured, and network parameters such as packet size, protocol type, and Traffic volume are extracted.

Step 2: Data Preprocessing: Missing or corrupted records are removed from the dataset. Categorical features are converted into numerical values, and normalisation is applied to scale the data.

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

where X represents the original feature value, X_{min} represents the minimum value, and X_{max} represents the maximum value.

Step 3: Feature Extraction: Relevant network traffic features are extracted and represented as a feature vector:

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \quad (2)$$

where f_i represents network parameters such as traffic volume, packet variance, TCP window size, ICMP type, HTTP request method, and packet transmission rate.

Step 4: Dataset Splitting: The dataset is divided into training and testing datasets:

$$D = D_{train} + D_{test} \quad (3)$$

Typically, 80% of the data is used for training and 20% for testing.

Step 5: Model Training: Multiple machine learning algorithms are trained using the training dataset, including Decision Tree, Support Vector Machine, Random Forest, and Gradient Boosting classifiers.

The classification function is expressed as:

$$Y = f(F) \quad (4)$$

where F represents the feature vector and Y represents the predicted traffic class.

Step 6: Intrusion Detection: The trained model analyses incoming network traffic. If abnormal traffic patterns are detected, the traffic is classified as malicious; otherwise, it is classified as normal.

Step 7: Performance Evaluation: Model performance is evaluated using common metrics such as accuracy, precision, recall, and F1-score.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (5)$$

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

$$Recall = \frac{TP}{TP + FN} \quad (7)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (8)$$

Step 8: Intrusion Alert System: When malicious traffic is detected, the system generates an alert to the control server, blocks suspicious packets, and records the event for future security analysis.

IV. METHODOLOGY

The proposed methodology focuses on designing an AI-based Intrusion Detection System (IDS) for drone communication networks. The system analyses network traffic generated between drones, ground control stations, and cloud servers to identify malicious activities and abnormal communication patterns. The methodology integrates data preprocessing, feature extraction, machine learning model training, intrusion detection, and performance evaluation to ensure accurate detection of cyber threats in drone networks.

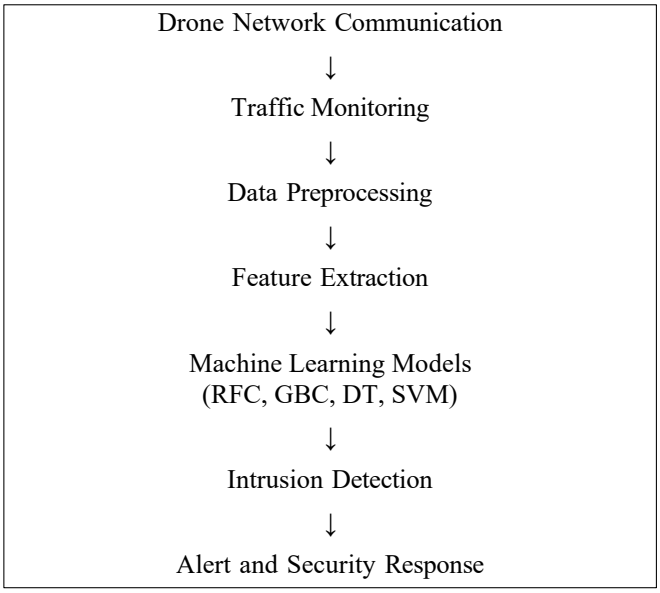

Fig. 1. AI-Based Intrusion Detection Architecture for Drone Networks

A. System Architecture

The proposed intrusion detection framework consists of several components, including data acquisition, preprocessing, feature extraction, machine learning classification, and alert generation. The system continuously monitors drone communication traffic and processes it through machine learning models to detect suspicious activities.

Drone communication networks typically involve Unmanned Aerial Vehicles (UAVs), ground control stations, communication gateways, and cloud infrastructure. These components exchange data packets through wireless communication protocols such as TCP/IP, HTTP, and ICMP. Since drone networks operate in open environments, they are vulnerable to attacks such as spoofing, packet injection, jamming, denial-of-service (DoS), and unauthorized access.

The proposed AI-based intrusion detection system monitors network traffic and analyses communication behavior to identify anomalies and potential cyber threats.

B. Data Collection

The first stage involves collecting network traffic data from drone communication systems. The dataset contains various network parameters that represent communication behavior between drones and control servers.

The collected dataset includes the following features:

- Traffic volume
- Packet size variance
- TCP window size
- ICMP type
- HTTP request method

- Request frequency
- Network latency
- Packet transmission rate

These features provide critical information about network traffic behaviour and help identify abnormal communication patterns.

C. Data Preprocessing

Raw network traffic data often contains missing values, redundant entries, and inconsistent formats. Therefore, preprocessing is necessary to improve the quality of the dataset before applying machine learning algorithms.

The preprocessing steps include:

- Data cleaning by removing incomplete or corrupted records
- Data transformation by converting categorical features into numerical form
- Feature normalisation to scale data values

The normalisation process is defined as:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (9)$$

where X represents the original feature value, X_{min} represents the minimum value, and X_{max} represents the maximum value.

D. Feature Extraction

Feature extraction is used to identify important network traffic parameters that influence intrusion detection. The extracted features are represented as a feature vector:

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \quad (10)$$

where each f_i represents a network feature such as traffic volume, packet size variance, TCP window size, ICMP type, or HTTP request type.

Feature selection reduces computational complexity and improves model performance.

E. Machine Learning Model Training

After preprocessing and feature extraction, the dataset is divided into training and testing datasets.

$$D = D_{train} + D_{test} \quad (11)$$

Typically, 80% of the dataset is used for training and 20% for testing.

The following machine learning algorithms are used in the proposed intrusion detection system:

- Random Forest Classifier (RFC)
- Gradient Boosting Classifier (GBC)
- Decision Tree (DT)
- Support Vector Machine (SVM)

The classification function can be expressed as:

$$Y = f(F) \quad (12)$$

where F represents the feature vector and Y represents the predicted traffic class (Normal or Intrusion).

F. Intrusion Detection Process

After training the machine learning models, incoming drone network traffic is analysed in real time. The extracted network features are fed into the trained models to classify the traffic.

If abnormal communication patterns are detected, the traffic is classified as malicious, and an intrusion alert is generated.

G. Intrusion Alert and Response

When malicious traffic is detected, the system performs several actions:

- Generates an alert to the drone control server
- Blocks suspicious communication packets
- Logs attack information for security analysis
- Prevents unauthorised commands from reaching the drone

H. Performance Evaluation

The performance of the intrusion detection system is evaluated using standard machine learning metrics.

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (13)$$

Precision

$$Precision = \frac{TP}{TP + FP} \quad (14)$$

Recall

$$Recall = \frac{TP}{TP + FN} \quad (15)$$

F1 Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (16)$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

The evaluation results help determine the effectiveness of the machine learning models in detecting intrusions within drone communication networks.

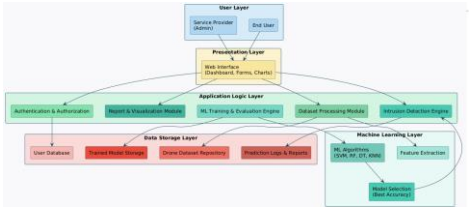

Fig. 2. Architecture Overview

V. RESULT ANALYSIS

This section presents the experimental results and performance evaluation of the proposed AI-based Intrusion Detection System (IDS) for drone communication networks. The objective of the evaluation is to analyse the effectiveness of different machine learning models in detecting malicious network traffic within UAV communication systems. The performance of the system is measured using several evaluation metrics, including accuracy, precision, recall, F1-score, and detection efficiency.

The intrusion detection framework was trained and tested using a dataset containing network traffic features such as traffic volume, packet size variance, TCP window size, ICMP type, HTTP request method, request frequency, and network latency. These features help in identifying abnormal traffic behaviour and distinguishing malicious activities from legitimate drone communication.

A. Model Performance Evaluation

The proposed system evaluates four machine learning models:

- Random Forest Classifier (RFC)
- Gradient Boosting Classifier (GBC)
- Decision Tree (DT)
- Support Vector Machine (SVM)

Each model was trained using the training dataset and tested using the testing dataset. The models classify network traffic as either normal communication or intrusion traffic.

Among the evaluated algorithms, Random Forest and Gradient Boosting classifiers demonstrated higher detection accuracy and better stability in dynamic network environments. These ensemble learning methods combine multiple decision trees, which improves classification performance and reduces the risk of overfitting.

Decision Tree models provided relatively fast classification but showed slightly lower accuracy when compared to ensemble methods. Support Vector Machines achieved strong classification performance but required higher computational resources time during training.

B. Detection Accuracy Analysis

The accuracy of each machine learning model was measured to evaluate its ability to correctly classify network traffic. Accuracy represents the ratio of correctly predicted instances to the total number of predictions.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

where:

- TP = True Positive
- TN = True Negative
- FP = False Positive
- FN = False Negative

Experimental results show that Random Forest and Gradient Boosting classifiers achieve the highest accuracy levels, making them more suitable for real-time drone network intrusion detection systems.

C. Precision and Recall Analysis

Precision and recall metrics are used to evaluate the reliability of intrusion detection models.

$$Precision = \frac{TP}{TP + FP} \tag{18}$$

$$Recall = \frac{TP}{TP + FN} \tag{19}$$

High precision indicates that the system generates fewer false alarms, while high recall indicates that most attacks are successfully detected. The experimental analysis shows that ensemble learning models provide better precision and recall compared to single classifier models.

D. F1 Score Evaluation

The F1 score combines precision and recall into a single metric that reflects the overall detection performance of the model.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{20}$$

The F1 score analysis confirms that Random Forest and Gradient Boosting classifiers outperform Decision Tree and Support Vector Machine models, achieving a better balance between attack detection and false alarm reduction.

E. False Positive and False Negative Analysis

In intrusion detection systems, minimising false positives and false negatives is crucial for maintaining reliable drone communication. A false positive occurs when normal network traffic is incorrectly classified as malicious, while a false negative occurs when an actual attack is not detected by the system.

The proposed framework significantly reduces the rate of false positives by using ensemble learning algorithms such as Random Forest and Gradient Boosting. These models analyse multiple decision paths and combine predictions to improve classification reliability.

F. Detection Rate Analysis

The attack detection rate measures the system's ability to correctly identify malicious traffic.

$$Detection\ Rate = \frac{TP}{TP + FN} \quad (21)$$

The experimental results indicate that the proposed AI-based intrusion detection framework achieves a high detection rate due to the combination of effective feature extraction and multiple machine learning models.

G. Real-Time Performance Evaluation

Drone networks require real-time monitoring because communication between drones and control stations must occur with minimal delay. The proposed system analyses incoming traffic packets in real time and classifies them using a trained machine learning model.

The system is capable of detecting attacks such as unauthorised command injection, packet manipulation, and denial-of-service attempts without introducing significant communication latency.

H. Scalability Analysis

As the number of drones in a network increases, the communication traffic also increases. The proposed intrusion detection framework is designed to handle large-scale datasets and dynamic network environments.

Machine learning models such as Random Forest and Gradient Boosting can process large volumes of traffic data efficiently, making the system suitable for large drone fleets and distributed UAV communication networks.

I. Overall System Effectiveness

The experimental results demonstrate that the proposed AI-based intrusion detection framework significantly improves the security of drone communication networks. By combining multiple machine learning algorithms with traffic analysis techniques, the system provides an intelligent and adaptive approach for detecting cyber threats in UAV systems.

The proposed system offers the following advantages:

- Accurate detection of malicious drone network traffic
- Reduced false alarm rates
- Improved communication reliability
- Enhanced protection against UAV cyber attacks
- Scalability for large drone network deployments

J. Experimental Setup

The dataset was divided into training (80%) and testing (20%) subsets. Supervised learning models including Linear Regression, Random Forest, and Gradient Boosting were trained and evaluated. Hyperparameter tuning was performed using cross-validation.

K. Performance Metrics

The performance of the models was evaluated using the following metrics:

1) Mean Absolute Error (MAE):

$$MAE = \frac{1}{n}\sum_{i=1}^{n} |E_{actual,i} - E_{pred,i}| \quad (22)$$

Example:

$$MAE = \frac{|12-11| + |15-16| + |18-17|}{3} = 1 \text{ kWh} \quad (23)$$

2) Root Mean Square Error (RMSE):

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n} (E_{actual,i} - E_{pred,i})^2} \quad (24)$$

Example:

$$RMSE = \sqrt{\frac{(1)^2 + (-1)^2 + (1)^2}{3}} = 1 \text{ kWh} \quad (25)$$

3) Coefficient of Determination (R^2):

$$R^2 = 1 - \frac{\sum_{i=1}^{n} (E_{actual,i} - E_{pred,i})^2}{\sum_{i=1}^{n} E_{actual,i} - \bar{E}_{actual}^{\ 2}} \quad (26)$$

An R^2 value close to 1 indicates better predictive performance.

L. Energy Consumption Model

The general energy prediction model is expressed as:

$$E = f(v, a, d, T, SOC, G) \quad (27)$$

where v is vehicle speed, a is acceleration, d is distance traveled, T is ambient temperature, SOC is state of charge, and G is road gradient.

1) Linear Regression Model:

$$E = \beta_0 + \beta_1 v + \beta_2 a + \beta_3 d + \beta_4 T + \beta_5 SOC + \beta_6 G \quad (28)$$

Example Calculation:

Given:

$$\beta_0 = 2.5, \quad \beta_1 = 0.04, \quad \beta_2 = 0.6, \quad \beta_3 = 0.03, \quad \beta_4 = 0.02,$$

For input values:

$$v = 50, \quad a = 1.5, \quad d = 10, \quad T = 30, \quad SOC = 80, \quad G = 2$$

International Journal of Engineering Research and Science & Technology

$$E = 2.5+(0.04)(50)+(0.6)(1.5)+(0.03)(10)+(0.02)(30)-(0.01)(80) \quad (29)$$

$$E = 6.5 \text{ kWh} \quad (30)$$

M. Model Comparison

TABLE I
MODEL PERFORMANCE COMPARISON

Model	MAE (kWh)	RMSE (kWh)	R^2
Linear Regression	1.35	1.80	0.84
Random Forest	0.92	1.25	0.90
Gradient Boosting	0.85	1.10	0.93

The results show that ensemble-based models outperform linear regression in terms of prediction accuracy. Gradient Boosting achieved the highest R^2 value, indicating superior generalisation performance.

Visualization and Output:

Fig. 3. wed page

Fig. 4. login page

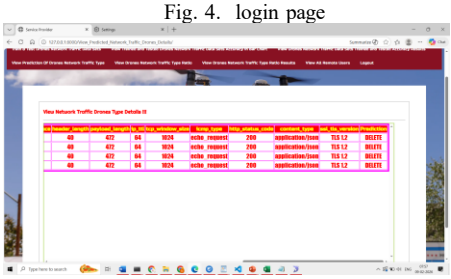

Fig. 5. Predicted value

Fig. 6. Accuracy Results

VI. CONCLUSION

The rapid growth of drone (UAV) networks in applications such as surveillance, delivery systems, disaster monitoring, and remote sensing has introduced significant cybersecurity challenges. Since drone communication relies heavily on wireless networks and real-time data exchange, these systems are highly vulnerable to cyber threats, including spoofing attacks, packet injection, denial-of-service attacks, and unauthorised access. Therefore, implementing intelligent and adaptive security mechanisms is essential for ensuring safe and reliable drone operations.

This research presented an AI-based intrusion detection system for drone communication networks using machine learning techniques. The proposed framework analyzes network traffic data and identifies abnormal communication patterns to detect potential cyber attacks. Several machine learning algorithms, including Random Forest Classifier (RFC), Gradient Boosting Classifier (GBC), Decision Tree (DT), and Support Vector Machine (SVM), were evaluated for their effectiveness in classifying network traffic and detecting intrusions.

Experimental analysis demonstrates that ensemble learning models such as Random Forest and Gradient Boosting provide higher detection accuracy, improved stability, and better performance in dynamic network environments compared to individual classifiers. The system effectively detects malicious traffic while reducing false alarm rates and maintaining efficient communication between drones and control servers.

Furthermore, the proposed framework enhances overall drone network performance by reducing packet loss, improving communication reliability, and enabling real-time threat detection. The integration of artificial intelligence into drone communication security provides an adaptive and scalable solution capable of identifying both known and emerging cyber threats.

In conclusion, the proposed AI-based intrusion detection framework significantly improves the security and efficiency of UAV communication networks. Future work can focus on integrating deep learning techniques, edge computing, and real-time distributed monitoring systems to further enhance intrusion detection accuracy and scalability in large-scale

drone networks.

VII. Future Scope:

The proposed AI-Based Intrusion Detection System (IDS) for Drone Networks provides an effective approach for identifying malicious activities in UAV communication systems. However, as drone technology continues to evolve and drone networks become more complex, several improvements and extensions can be explored in future research to enhance the system's performance, scalability, and security capabilities.

One important future direction is the integration of deep learning techniques such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks. These models are capable of analyzing complex traffic patterns and temporal network behaviors, which can improve the accuracy of intrusion detection in highly dynamic drone communication environments.

Another promising area is the use of edge computing and fog computing for real-time intrusion detection. Instead of sending all network traffic data to centralized servers, security analysis can be performed at edge devices or drone gateways. This approach can significantly reduce communication latency and enable faster detection of cyber threats in real-time drone operations.

Future work can also explore the integration of blockchain technology to enhance the security and integrity of drone communication networks. Blockchain can provide decentralized authentication, secure data sharing, and tamper-proof logging of drone communication activities, which can further strengthen the overall cybersecurity framework.

In addition, the system can be extended to support large-scale drone swarm networks, where multiple drones operate simultaneously and generate large volumes of network traffic. Advanced machine learning models and distributed detection mechanisms will be required to efficiently monitor and secure such complex networks.

Another potential improvement involves developing adaptive intrusion detection models that continuously learn from new attack patterns using online learning techniques. This would allow the system to detect previously unknown cyber attacks and respond effectively to emerging security threats.

Finally, future research can focus on improving the energy efficiency and computational optimization of machine learning models so that intrusion detection mechanisms can be deployed directly on lightweight drone hardware without significantly affecting system performance.

Overall, incorporating advanced AI techniques, distributed computing technologies, and scalable security frameworks will further enhance the effectiveness of AI-based intrusion detection systems for secure and reliable drone communication networks.

References

[1] M. Gamal, A. Tharwat, and A. E. Hassanien, "Improving intrusion detection using LSTM-RNN to protect drone communication," Egyptian Informatics Journal, vol. 27, pp. 100–112, 2024.https://www.sciencedirect.com/science/article/pii/S1110866524000641

[2] S. Miao, Y. Zhang, and X. Liu, "Unmanned aerial vehicle intrusion detection using deep CNN-BiLSTM with attention," Internet of Things, vol. 25, 2024.https://www.sciencedirect.com/science/article/pii/S2214209624000019

[3] Y. Wu, L. Yang, and L. Nie, "Intrusion detection for unmanned aerial vehicles security: A tiny machine learning model," IEEE Internet of Things Journal, 2024.https://doi.org/10.1109/JIOT.2024.3360231

[4] S. Menssouri, M. Delamou, and K. Ibrahimi, "Enhanced intrusion detection system for multiclass classification in UAV networks," 2024.https://arxiv.org/abs/2406.10417

[5] H. J. Hadi et al., "Real-time collaborative intrusion detection system in UAV networks," Iraqi Journal for Information Technology, 2024.https://ui.adsabs.harvard.edu/abs/2024IITJ...1133371J/abstract

[6] W. Zhou et al., "Intrusion detection model of UAV system based on machine learning and neural networks," Frontiers in Physics, vol. 13, 2025.https://www.frontiersin.org/articles/10.3389/fphy.2025.1660104

[7] J. Medhi, R. Liu, and X. Chen, "A lightweight and efficient intrusion detection system for unmanned aerial vehicles," Neural Computing and Applications, 2025.https://link.springer.com/article/10.1007/s00521-025-11276-5

[8] T. Wisanwanichthan et al., "A lightweight intrusion detection system for IoT and UAV using knowledge distillation," Computers, vol. 14, no. 7, 2025.https://www.mdpi.com/2073-431X/14/7/291

[9] M. D. S. Islam et al., "AI-enhanced intrusion detection for UAV systems," Drones, vol. 9, no. 10, 2025.https://www.mdpi.com/2504-446X/9/10/682

[10] Q. Zeng, A. Bashir, and F. Nait-Abdesselam, "UAVIDS-2025: A benchmark dataset for intrusion detection in UAV networks using machine learning

techniques," in Proc. IEEE CNS, 2025.https://doi.org/10.1109/CNS66487.2025.11194990

[11] T. K. Biswas et al., "A lightweight temporal-spatial transformer approach for intrusion detection in drone networks," 2025.https://arxiv.org/abs/2510.02711

[12] D. K. Panda and W. Guo, "Generative adversarial evasion and out-of-distribution detection for UAV cyber-attacks," 2025.https://arxiv.org/abs/2506.21142

[13] A. Khanfor, R. Hamadi, and N. Lasla, "AI-driven intrusion detection for UAV in smart urban ecosystems: A comprehensive survey," 2026.https://arxiv.org/abs/2601.19345

[14] "Machine learning-based intrusion detection systems for the Internet of Drones: A systematic literature review," 2025.https://www.researchgate.net/publication/392250763

[15] "ML-based intrusion detection for drone IoT security," Journal of Cybersecurity and Information Management, 2024.https://www.americaspg.com/articleinfo/2/show/2843