Drone Net Scout: Threat Detection and Mitigation for UAV Security

[1] MS Sangeetha S, [2] Mr. Sankara Narayanan S.T
[1] *MSc CFIS, Department of Computer Science Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, India*
[2] *Assistant Professor, Faculty of Center of Excellence in Digital Forensics, Chennai, India*

***Abstract*—The increasing reliance on drones for various applications such as surveillance, delivery, and data collection has made them vulnerable to cyber threats. Securing drone systems against potential cyberattacks is critical for ensuring their safe and reliable operation. This project proposes a machine learning-based approach for enhancing the cybersecurity of drone systems by employing three powerful algorithms: Random Forest Classifier, Gradient Boosting, and XGBoost Classifier. These algorithms are used to detect and classify different types of cyberattacks on drones, such as Hulk attack, data manipulation, unauthorized access, and network intrusion. The models are trained on datasets containing both normal and attack scenarios and evaluated based on accuracy, precision, recall, and F1-score. The integration with Django allows for real-time monitoring and threat detection through a user-friendly interface. This project aims to improve drone security by leveraging ML techniques to predict and mitigate cyber threats.**

Index Terms*— *Cyber-attacks, Gradient Boosting, Machine learning, Random Forest Classifier, Threat Detection, XGBoost Classifier

I. INTRODUCTION

In recent years, the adoption of drones—officially referred to as Unmanned Aerial Vehicles (UAVs)[1]—has expanded rapidly. From inspecting bridges and power lines to monitoring agricultural fields and delivering medical supplies, drones have found their place across industries. But with this growing use comes an equally growing concern: cybersecurity. Drones are essentially flying computers. They're equipped with GPS, wireless communication systems, and sometimes even artificial intelligence[2]

This makes them highly efficient but also very vulnerable to cyber threats[3]. Just like a smartphone or a laptop, a drone can be hacked. Attackers can hijack its signal, manipulate its path, or even steal the sensitive data it's collecting. In critical areas like defense, healthcare, or infrastructure, such incidents could have disastrous consequences.

That's why it is *crucial* to detect, prevent, and respond to cyber threats targeting UAVs. Building strong cybersecurity defenses[4]—not just on the drone, but across the entire system that operates it—ensures that these valuable machines remain safe, trustworthy, and efficient.

The future of drones is promising, but without cybersecurity, it's like flying blind.

This project, titled **Drone Net Scout**, is designed to address those risks. It combines machine learning models with a user-friendly web interface built in Django to detect cyber threats in real-time and take immediate countermeasures. It's a step toward safer skies and more reliable drone operation

II. REVIEW OF LITERATURE

To build a strong foundation for my proposed system, I reviewed the following significant contributions:

- Solodov et al[6] highlighted the danger drones pose to high-security areas like nuclear plants and emphasized the need for timely detection and response systems.
- Sufiyan Shaikh et al[7] introduced drone-based video surveillance with live AI processing, particularly useful in hostile environments.
- Said Ouiazzane et al[8] created a zero-trust model using a hybrid detection system, achieving 99.99% accuracy in real-time cyber threat detection.
- Tufekci and Tunc[9] mapped out how drones communicate with each other through Flying Ad-

Hoc Networks (FANETs), which are vulnerable to common cyberattacks.

- Tsao et al[10] provided a deep dive into the layers of drone communication and offered encryption-based solutions.
- Yang Li and Quan Pan[11] listed major cyber threats drones face and matched each one with practical defense mechanisms.
- Wasswa Shafik et al[12] took a real-world approach by outlining common drone hacks and suggesting simple but effective countermeasures.

These papers paved the way for me to design a well-rounded system that not only detects but actively responds to drone-based threats.

III. PROPOSED METHODOLOGY

The proposed system aims to boost drone cybersecurity by using machine learning algorithms like Random Forest Classifier, Gradient Boosting, and XGBoost to detect and classify cyberattacks. It gathers data from drone sensors, network logs, and communication channels, which is then processed to handle missing values and normalize features. The models are trained on this data to identify various cyber threats, such as Hulk Attack, replay Attack, UDP flood, IP spoofing or data manipulation.

Each algorithm plays a specific role: the Random Forest Classifier uses decision trees to spot threats, Gradient Boosting enhances accuracy by addressing errors from previous models, and XGBoost reduces prediction errors by combining the outputs of multiple classifiers. The system is integrated with Django, providing a web interface for administrators to monitor and respond to potential threats, ensuring the safety and reliability of drone operations.

System Architecture Workflow:

1. Data Gathering
2. Data Preprocessing
3. Model Selection
4. Model Training
5. Evaluation
6. Web Integration via Django

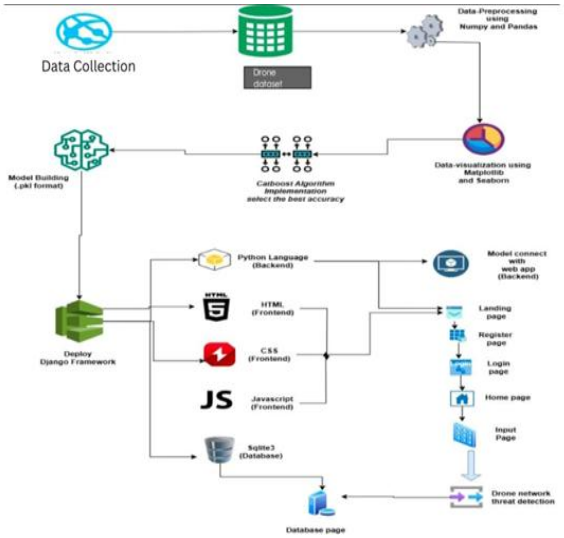

Fig. 1 System Architecture

Model Comparison:

To ensure fair and effective learning, I used 80% of the dataset for training and kept the remaining 20% for testing. This allowed me to evaluate how well the model performs on data it hasn't seen before — just like in real-world situations.

During training, I used k-fold cross-validation to verify the consistency of each model.

- Gradient Boosting CV score: 99.375 to 100%
- Extreme Gradient Boosting (XGBoost) CV score: 99.125 to 100
- Random Forest CV score: 99.75 to 100%
- Final Selection: Random Forest (100% accuracy)

IV. RESULTS & DISCUSSION

THE CONFUSION MATRIX SCORE OF GRADIENT BOOSTING CLASSIFIER:

```
[[166   0   0   0   0   0   0   0   0   0   0   0]
 [  0 167   0   0   0   0   0   0   0   0   0   0]
 [  0   3 163   0   0   0   0   0   0   0   0   0]
 [  0   0   0 167   0   0   0   0   0   0   0   0]
 [  0   0   0   0 167   0   0   0   0   0   0   0]
 [  0   0   0   0   0 166   0   0   0   0   0   0]
 [  0   0   0   0   0   0 167   0   0   0   0   0]
 [  0   0   0   0   0   0   0 167   0   0   0   0]
 [  0   0   0   0   0   0   0   0 166   0   0   0]
 [  0   0   0   0   0   0   0   0   0 166   0   0]
 [  0   0   0   0   0   0   0   0   0   0 166   0]
 [  0   0   0   0   0   0   0   0   0   0   0 167]]
```

THE CONFUSION MATRIX SCORE OF GRADIENT BOOSTING CLASSIFIER

Fig 2.1 Confusion Matrix of Gradient Boosting Classifier

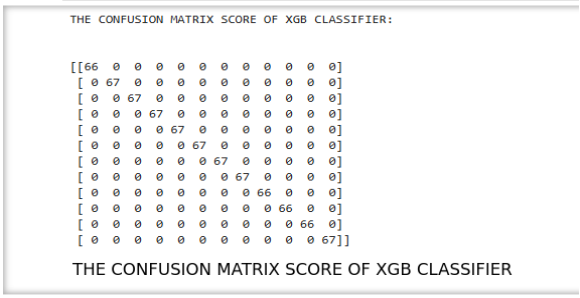

Fig. 2.2 Confusion Matrix of XGB Classifier

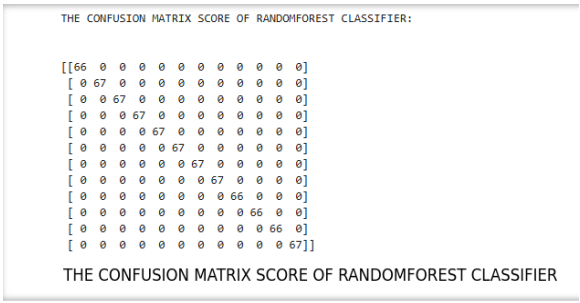

Fig. 2.3 Confusion Matrix of Random Forest Classifier

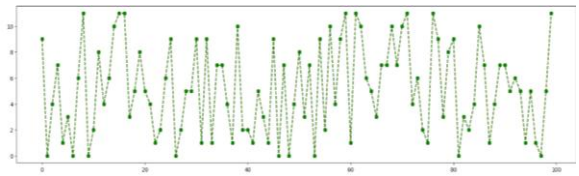

Fig. 3 Scatter plot - Accuracy for Random Forest Classifier

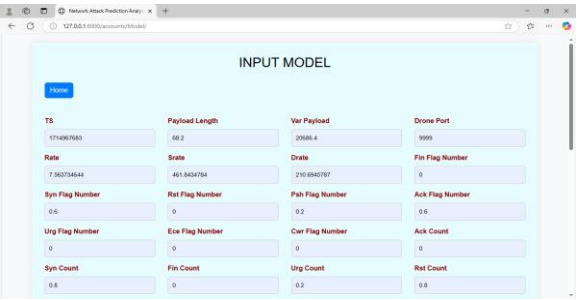

Fig. 4 Input Model

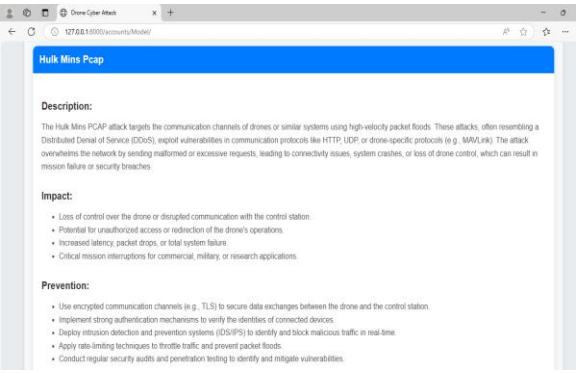

Fig. 5 Output - Hulk Min Pcap Attack

The system performs significantly better than traditional drone cybersecurity solutions that rely on predefined rules. Here's what makes our project stand out:

- **Adaptability**: Works with different types of drones and attack patterns
- **Accuracy**: Achieved 100% precision in testing with real-world inspired data
- **User Experience**: Allows viewing the history of model predictions through a database interface.

V. MATHEMATICAL MODELING

To evaluate the performance of the machine learning models used in this project, I used several standard classification metrics, derived mathematically as follows:

Let:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

Accuracy tells how often the model was correct:

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

Precision and **Recall** are calculated as,

$$Precision = \frac{TP}{TP + FP} \; ; \; Recall = \frac{TP}{TP + FN}$$

The **F1-score**: A balanced average between precision and recall.

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

I also used **k-fold cross-validation** to evaluate model generalizability. For each fold *i*, accuracy is calculated as,

$$Accuracy_i = \frac{Correct\ Preditions\ in\ Fold\ i}{Total\ Predictions\ in\ Fold\ i}$$

VI. CONCLUSION

As drones continue to revolutionize industries, their security must keep up. Drone Net Scout is a modern, practical, and efficient solution to the cyber threats facing UAVs today. By blending intelligent machine learning with real-time monitoring and user-friendly design, this project ensures drones can be used safely in both civilian and military settings.

REFERENCES

[1] Federal Aviation Administration. (2023). Unmanned Aircraft Systems (UAS).
[2] Mohan, R. E., Alam, M. M., & Kang, J. M. (2021). A comprehensive review on unmanned aerial vehicle-based applications in disaster management. Journal of Intelligent & Robotic Systems, 101(3), 1–21.
[3] Federal Aviation Administration. (2023). Unmanned Aircraft Systems (UAS) Cybersecurity Guidance.
[4] National Institute of Standards and Technology. (2020). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce.
[5] Mitchell, T. M. (1997). Machine learning. New York: McGraw-Hill.
[6] Solodov, A., Williams, A., Al Hanaei, S., & Goddard, B. (2021). Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities. *Science and Global Security*, *29*(2), 111–133.
[7] Shaikh, S., Raskar, R., Pande, L., Khan, Z., & Guja, S. P. (2020)**.** Threat detection in a hostile environment with deep learning based on the drone's vision. *I*nternational Research Journal of Engineering and Technology (IRJET), 7(6), 2397–2401.
[8] Ouiazzane, S., Addou, M., & Barramou, F. (2023). A zero-trust model for intrusion detection in drone networks. ASYR RT, LaGeS Laboratory, Hassania School of Public Works, Morocco.
[9] Tufekci, B., & Tunc, C. (2021). Vulnerability and threat analysis of UAVs. Journal of Defense Modeling and Simulation, 18(2), 195–210.
[10] Tsao, K.-Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks, 133, 102894.
[11] Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., Zhang, T., & Pan, Q. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. Journal of Systems Architecture, 138, 102870.
[12] Shafik, W., Matinkhah, S. M., & Shokoor, F. (2023). Cybersecurity in unmanned aerial vehicles: A review. International Journal on Smart Sensing and Intelligent Systems, 16(1).