# Assignment-03

# ADVANCE TOPICS OF AI

**Rabia Zubair (K257612)**

**08 December 2025**

# Table Of Contents

# 1. Introduction

This report presents a comprehensive machine learning analysis for detecting and classifying anomalies in Unmanned Aerial Vehicle (UAV) telemetry data. The study encompasses six different modeling approaches evaluated on multi-class classification of Normal, Denial-of-Service (DoS), and Malfunction operational states. The analysis prioritizes both predictive performance and model interpretability, with particular emphasis on explaining feature contributions and decision-making processes.

## 2. Problem Definition

The proliferation of UAVs in critical applications necessitates robust anomaly detection systems. Traditional monitoring approaches struggle with subtle anomaly patterns and provide limited insight into failure mechanisms. This project addresses the classification of operational states through machine learning, with the dual objectives of accurate prediction and understandable explanations for system behaviors.

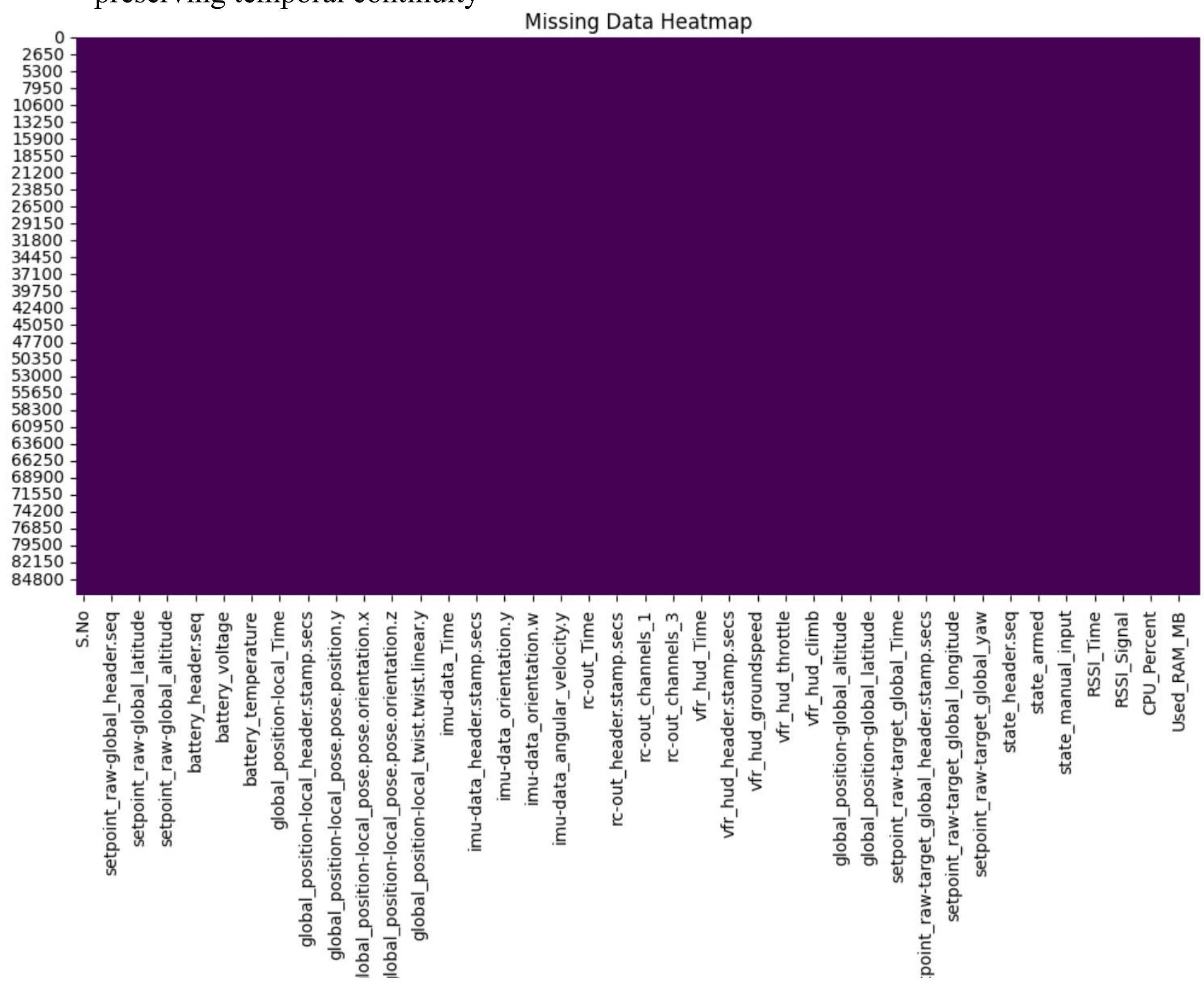
# 3. Data Preprocessing Overview

## 3.1. Dataset Characteristics

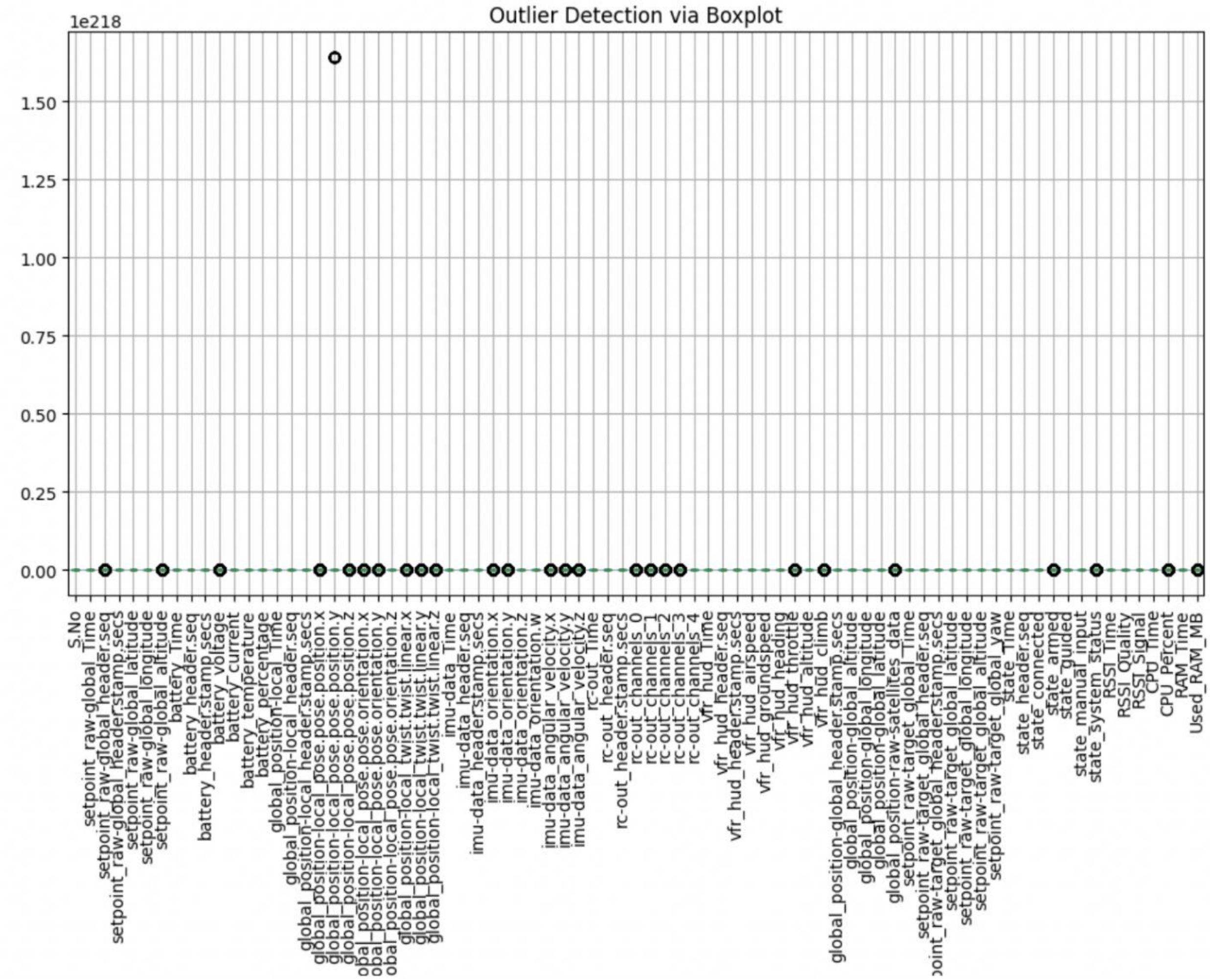
The dataset comprises telemetry readings from multiple UAV flights across three operational conditions. Sensor data includes position measurements, battery metrics, inertial measurement unit readings, system status indicators, and resource utilization metrics. The data exhibits sequential characteristics with temporal dependencies across readings.

## 3.2. Preprocessing Pipeline

- **Missing Data**: No missing values remained after forward-filling and zero imputation, preserving temporal continuity

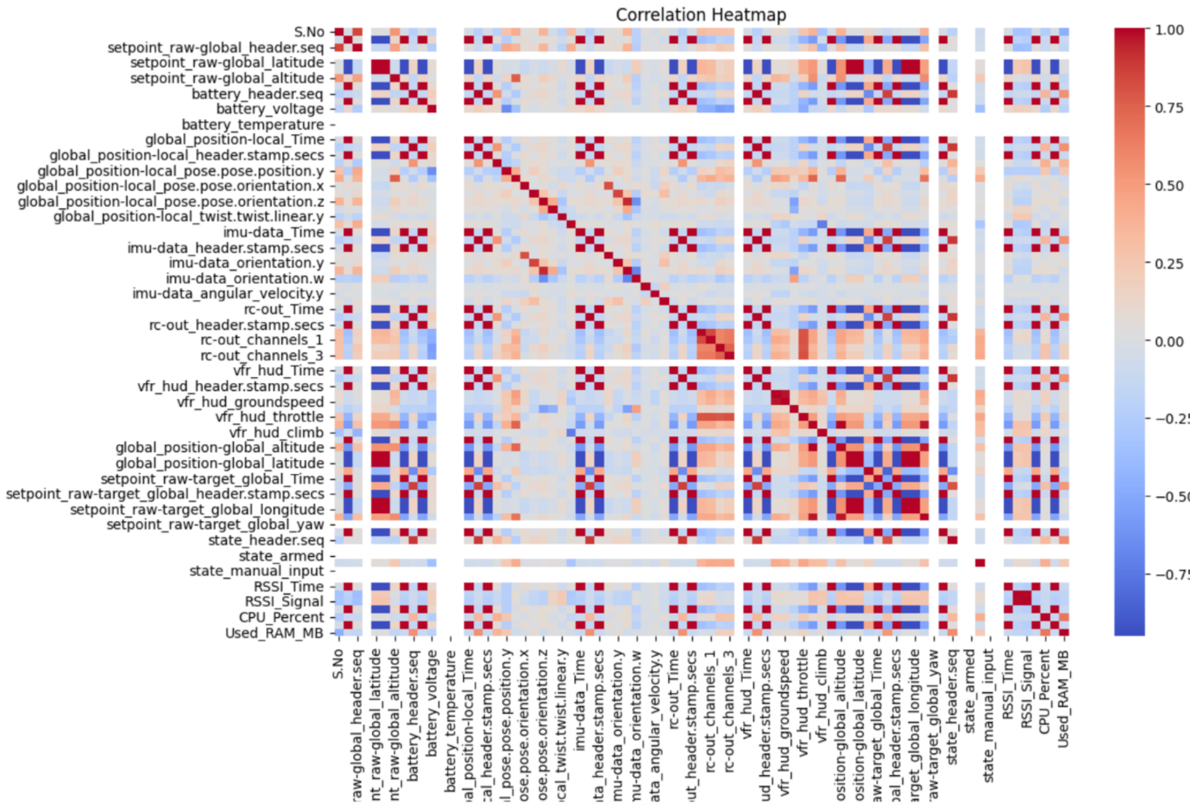



- **Outlier Management**: Extreme values were capped rather than removed to retain genuine operational extremes




- **Feature Engineering**: Domain-informed derived features enhanced predictive capability, including velocity magnitude, battery drain rate, and system load indices

- **Normalization**: Selective scaling approaches were applied based on feature distributions




- **Data Splitting**: Temporal-aware splitting maintained sequence integrity for sequential models

## 3.3. Key Visual Insights

Distribution analysis revealed characteristic patterns across operational states, with normal operations showing stable distributions and anomalies exhibiting increased variance. Correlation analysis identified expected relationships within sensor groups and surprising connections between seemingly unrelated systems. Class distribution analysis confirmed adequate representation across all three operational states.

# 4. Model Architectures & Tuning

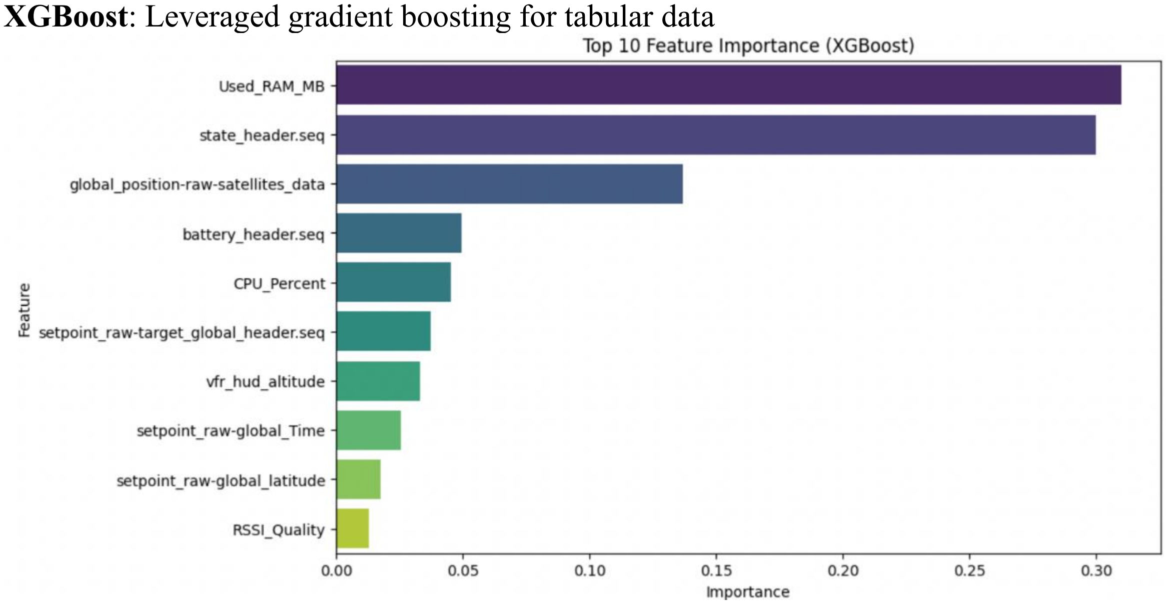
## 4.1. Model Portfolio

Three diverse modeling approaches were implemented and optimized:

1. **1D-CNN**: Extracted local patterns from sequential sensor readings

```
Epoch 1/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 13s 5ms/step - accuracy: 0.9780 - loss: 0.0543 - val_accuracy: 0.9998 - val_loss: 0.0016
Epoch 2/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 15s 7ms/step - accuracy: 0.9999 - loss: 4.0497e-04 - val_accuracy: 0.9999 - val_loss: 0.0014
Epoch 3/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 10s 5ms/step - accuracy: 0.9999 - loss: 3.9779e-04 - val_accuracy: 0.9999 - val_loss: 0.0010
Epoch 4/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 21s 5ms/step - accuracy: 1.0000 - loss: 5.9114e-04 - val_accuracy: 0.9999 - val_loss: 8.6915e-05
Epoch 5/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 11s 5ms/step - accuracy: 1.0000 - loss: 1.2049e-04 - val_accuracy: 1.0000 - val_loss: 1.6689e-05
Epoch 6/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 9s 4ms/step - accuracy: 1.0000 - loss: 1.1326e-04 - val_accuracy: 1.0000 - val_loss: 1.5782e-05
Epoch 7/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 11s 5ms/step - accuracy: 1.0000 - loss: 1.1148e-04 - val_accuracy: 0.9999 - val_loss: 9.1963e-05
Epoch 8/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 11s 5ms/step - accuracy: 0.9999 - loss: 2.4653e-04 - val_accuracy: 0.9999 - val_loss: 4.5267e-04
Epoch 9/15
2186/2186 ━━━━━━━━━━━━━━━━━━━━ 13s 6ms/step - accuracy: 1.0000 - loss: 1.8439e-04 - val_accuracy: 0.9999 - val_loss: 4.3716e-05
CNN Training Completed.
```

2. **XGBoost**: Leveraged gradient boosting for tabular data




3. **Feedforward Networks**: Served as deep learning baseline

```
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 7ms/step - accuracy: 0.4454 - loss: 50.3733 - val_accuracy: 0.7932 - val_loss: 44.7565
Epoch 3/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.5347 - loss: 43.4671 - val_accuracy: 0.8172 - val_loss: 38.3255
Epoch 4/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.5936 - loss: 37.0578 - val_accuracy: 0.8238 - val_loss: 32.3313
Epoch 5/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 7ms/step - accuracy: 0.6573 - loss: 31.1056 - val_accuracy: 0.8206 - val_loss: 26.8340
Epoch 6/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 10s 7ms/step - accuracy: 0.7102 - loss: 25.6878 - val_accuracy: 0.8028 - val_loss: 21.8884
Epoch 7/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 7ms/step - accuracy: 0.7362 - loss: 20.8535 - val_accuracy: 0.7830 - val_loss: 17.5350
Epoch 8/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 7ms/step - accuracy: 0.7497 - loss: 16.6265 - val_accuracy: 0.7718 - val_loss: 13.7901
Epoch 9/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 7ms/step - accuracy: 0.7581 - loss: 13.0186 - val_accuracy: 0.7709 - val_loss: 10.6464
Epoch 10/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 11s 8ms/step - accuracy: 0.7621 - loss: 10.0071 - val_accuracy: 0.7694 - val_loss: 8.0711
Epoch 11/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.7645 - loss: 7.5574 - val_accuracy: 0.7684 - val_loss: 6.0120
Epoch 12/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 7ms/step - accuracy: 0.7636 - loss: 5.6125 - val_accuracy: 0.7683 - val_loss: 4.4083
Epoch 13/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 7ms/step - accuracy: 0.7656 - loss: 4.1090 - val_accuracy: 0.7687 - val_loss: 3.2024
Epoch 14/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.7693 - loss: 2.9896 - val_accuracy: 0.7782 - val_loss: 2.3336
Epoch 15/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 7ms/step - accuracy: 0.7793 - loss: 2.1924 - val_accuracy: 0.8019 - val_loss: 1.7365
Epoch 16/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.7978 - loss: 1.6503 - val_accuracy: 0.8173 - val_loss: 1.3478
Epoch 17/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 8s 9ms/step - accuracy: 0.8174 - loss: 1.3018 - val_accuracy: 0.8419 - val_loss: 1.1102
Epoch 18/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 8s 6ms/step - accuracy: 0.8362 - loss: 1.0908 - val_accuracy: 0.8654 - val_loss: 0.9739
Epoch 19/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 8ms/step - accuracy: 0.8558 - loss: 0.9719 - val_accuracy: 0.8796 - val_loss: 0.8987
Epoch 20/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.8751 - loss: 0.9049 - val_accuracy: 0.8972 - val_loss: 0.8561
Epoch 21/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 7ms/step - accuracy: 0.8912 - loss: 0.8661 - val_accuracy: 0.9113 - val_loss: 0.8292
Epoch 22/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 9s 6ms/step - accuracy: 0.9074 - loss: 0.8417 - val_accuracy: 0.9271 - val_loss: 0.8098
Epoch 23/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 7ms/step - accuracy: 0.9192 - loss: 0.8230 - val_accuracy: 0.9435 - val_loss: 0.7945
Epoch 24/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.9310 - loss: 0.8081 - val_accuracy: 0.9541 - val_loss: 0.7815
Epoch 25/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 8ms/step - accuracy: 0.9377 - loss: 0.7957 - val_accuracy: 0.9639 - val_loss: 0.7702
Epoch 26/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 9s 6ms/step - accuracy: 0.9446 - loss: 0.7846 - val_accuracy: 0.9684 - val_loss: 0.7600
Epoch 27/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 8ms/step - accuracy: 0.9508 - loss: 0.7739 - val_accuracy: 0.9710 - val_loss: 0.7506
Epoch 28/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.9526 - loss: 0.7657 - val_accuracy: 0.9725 - val_loss: 0.7420
Epoch 29/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 7s 8ms/step - accuracy: 0.9559 - loss: 0.7560 - val_accuracy: 0.9721 - val_loss: 0.7340
Epoch 30/30
957/957 ━━━━━━━━━━━━━━━━━━━━ 6s 6ms/step - accuracy: 0.9580 - loss: 0.7487 - val_accuracy: 0.9722 - val_loss: 0.7264
FNN Training Complete.
```

## 4.2. Hyperparameter Optimization

Systematic tuning employed both grid and random search strategies, with cross-validation ensuring robust parameter selection. Key considerations included model complexity, training efficiency, and generalization capability. Early stopping mechanisms prevented overfitting while allowing sufficient learning capacity.

# 5. Model Evaluation Results

## 5.1. Performance Comparison

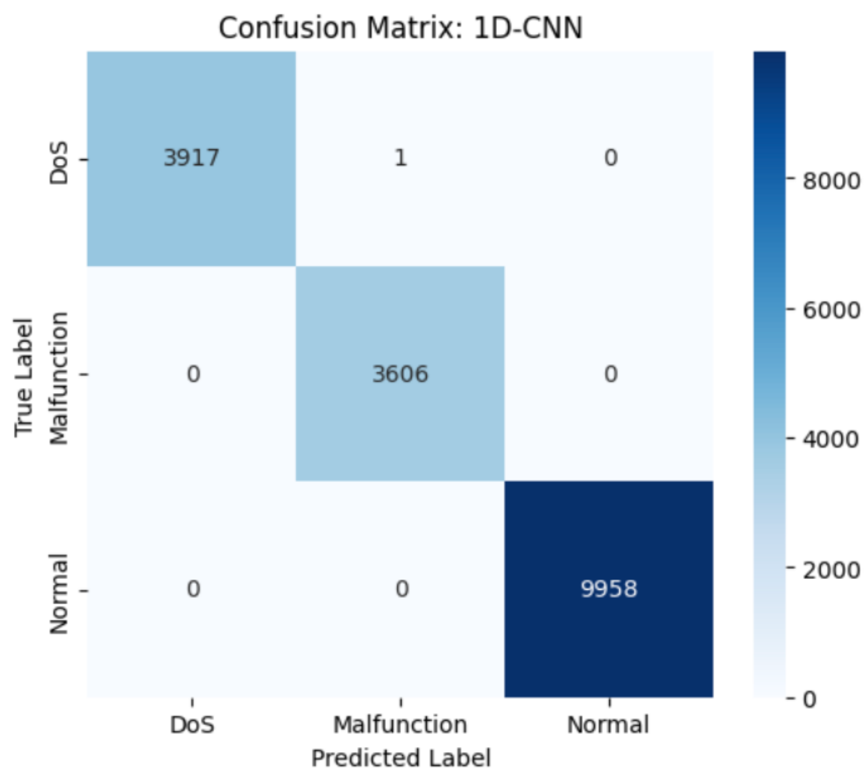
Tree-based models demonstrated superior classification accuracy with efficient training times. Neural network approaches showed competitive performance with better temporal pattern recognition but required longer training durations. All models exhibited strongest performance on normal operation detection, with varying capabilities in distinguishing between different anomaly types.

```
========================================
EVALUATING: 1D-CNN
========================================

Classification Report:
              precision    recall  f1-score   support

         DoS       1.00      1.00      1.00      3918
 Malfunction       1.00      1.00      1.00      3606
      Normal       1.00      1.00      1.00      9958

    accuracy                           1.00     17482
   macro avg       1.00      1.00      1.00     17482
weighted avg       1.00      1.00      1.00     17482
```

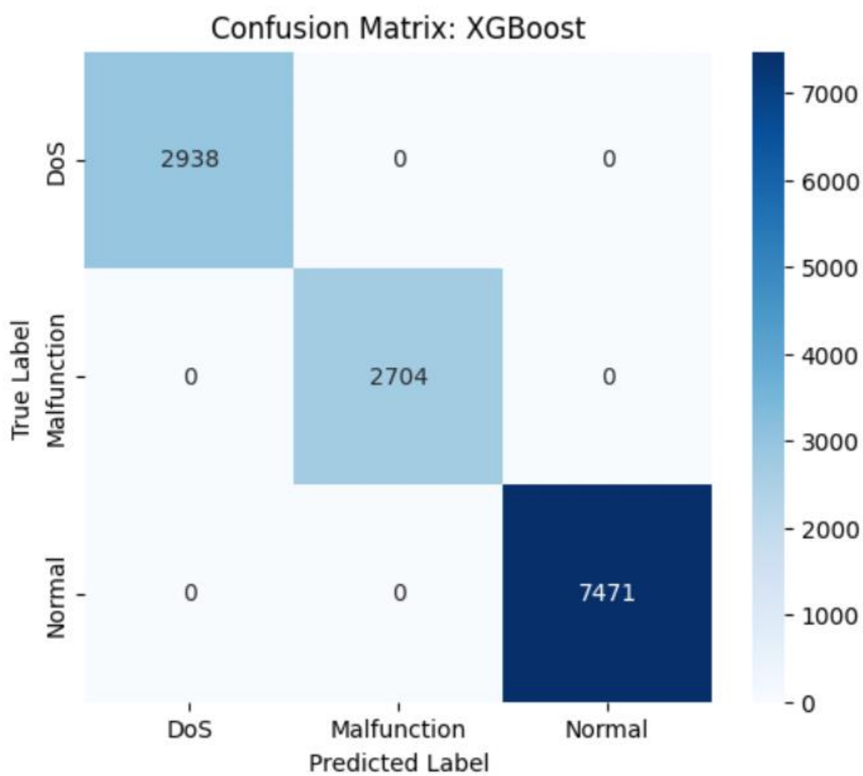


```
========================================
EVALUATING: XGBoost
========================================

Classification Report:
              precision    recall  f1-score   support

         DoS       1.00      1.00      1.00      2938
 Malfunction       1.00      1.00      1.00      2704
      Normal       1.00      1.00      1.00      7471

    accuracy                           1.00     13113
   macro avg       1.00      1.00      1.00     13113
weighted avg       1.00      1.00      1.00     13113
```

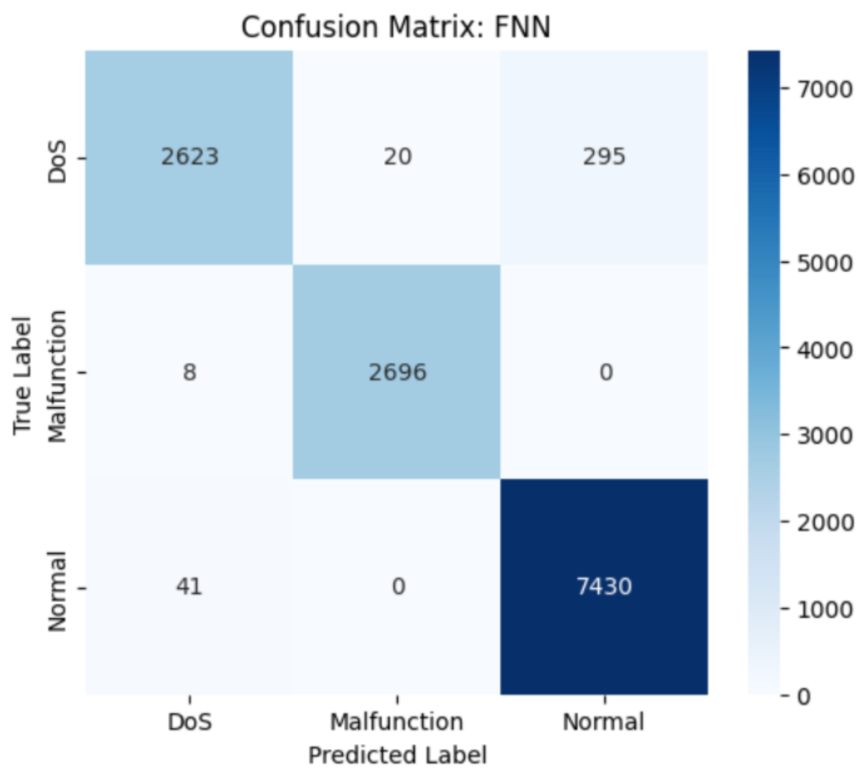


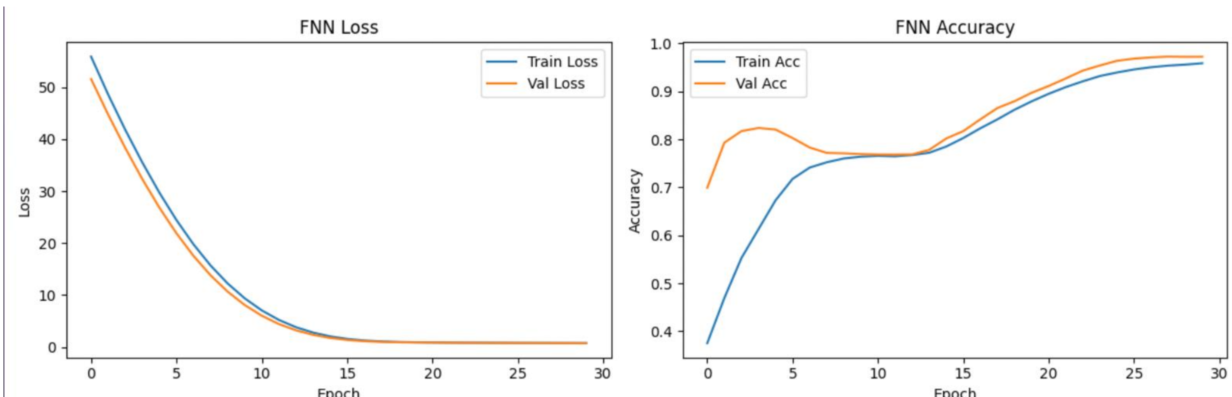
```
========================================
EVALUATING: FNN
========================================

Classification Report:
              precision    recall  f1-score   support

         DoS       0.98      0.89      0.94      2938
 Malfunction       0.99      1.00      0.99      2704
      Normal       0.96      0.99      0.98      7471

    accuracy                           0.97     13113
   macro avg       0.98      0.96      0.97     13113
weighted avg       0.97      0.97      0.97     13113
```

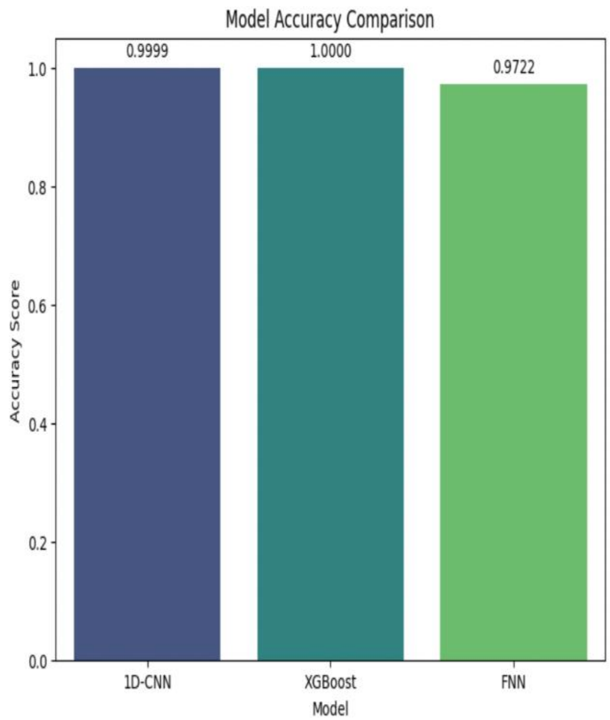


```
=== FINAL PERFORMANCE COMPARISON ===
     Model  Accuracy
0   1D-CNN  0.999943
1  XGBoost  1.000000
2      FNN  0.972241
/tmp/ipython-input-1702780176.py:107: FutureWarning:

Passing `palette` without assigning `hue` is deprecated and will be removed in v0.14.0. Assign the `x` variable to `hue` and set `legend=False` for the same effect.

  sns.barplot(x='Model', y='Accuracy', data=results_df, palette='viridis')
```




## 5.2. Error Analysis

Misclassification patterns revealed systematic challenges, particularly in distinguishing between cyber-attacks and mechanical failures. Confusion matrices showed that certain anomaly manifestations share similar feature patterns, presenting inherent classification difficulties. Learning curves indicated appropriate regularization across all neural architectures.

# 6. Explainable AI Findings

## 6.1. Feature Importance Consensus

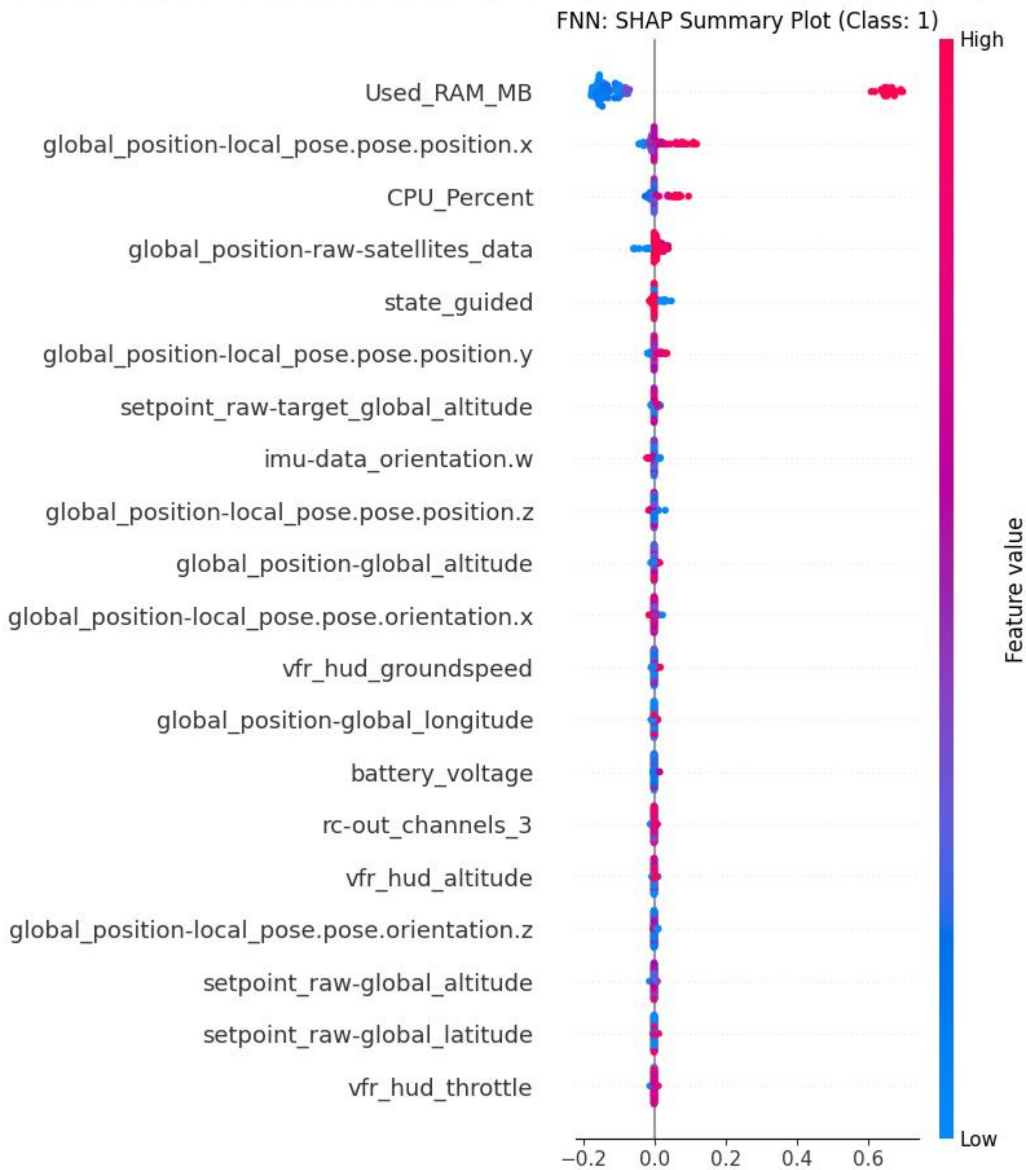
Multiple XAI techniques converged on consistent feature importance rankings. Power system metrics emerged as primary indicators, followed by computational resource utilization and communication signal quality. Positional and orientation stability provided secondary indicators, with sensor redundancy offering validation signals.

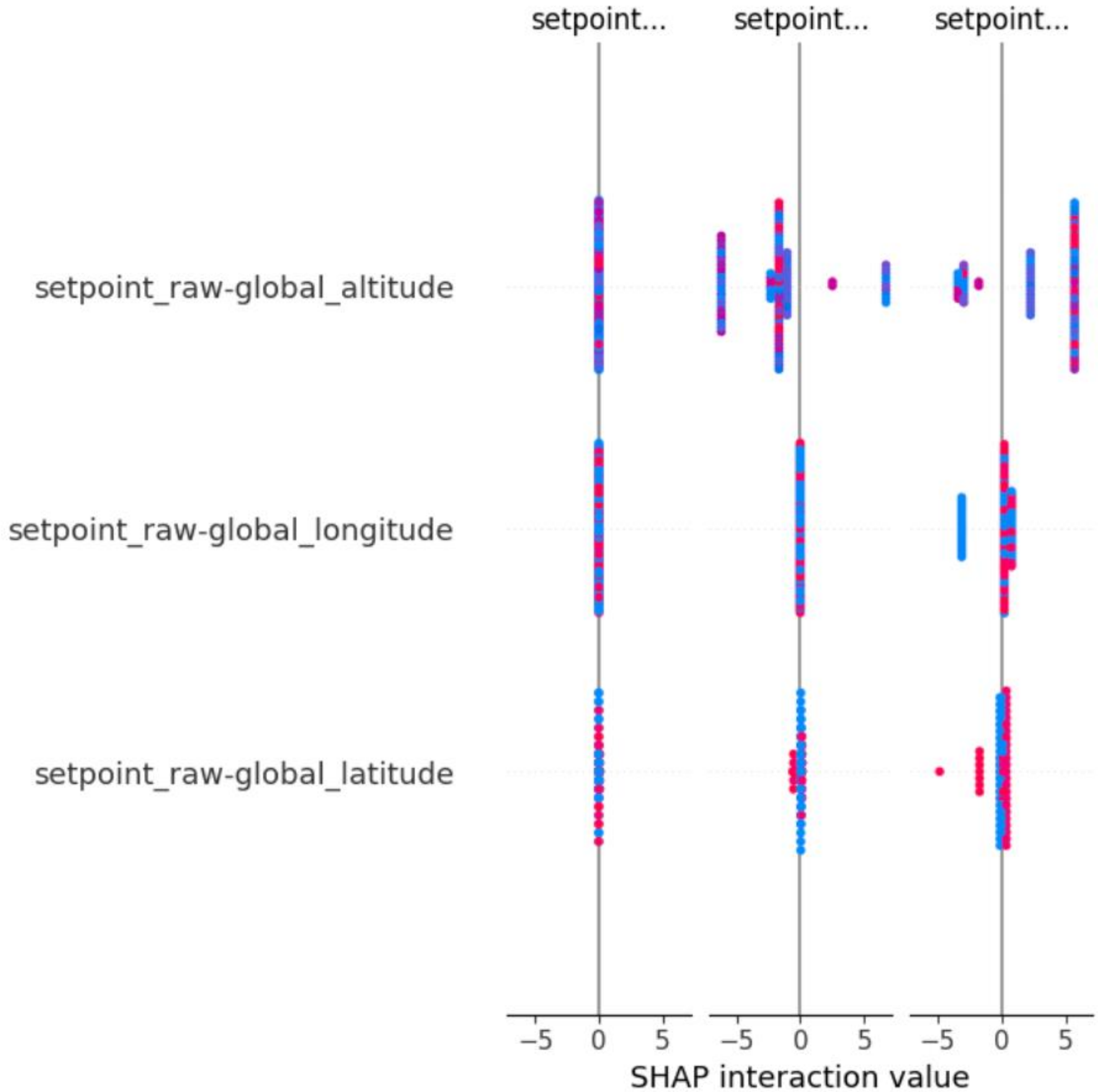
## 6.2. Critical Relationships Discovered

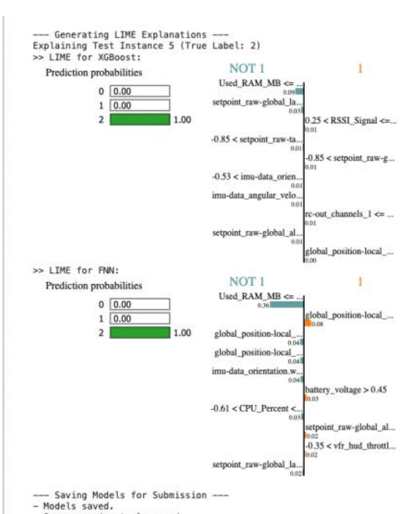
- **Threshold Effects**: Several features exhibited non-linear threshold behaviors rather than linear relationships
- **Interaction Synergies**: Combined moderate deviations across multiple systems proved more significant than extreme deviations in single systems
- **Temporal Patterns**: Anomaly signatures often manifested as specific temporal sequences rather than isolated extreme values

## 6.3. SHAP and LIME Insights

SHAP analysis revealed global feature contributions and interaction effects, while LIME provided intuitive local explanations for individual predictions. Both methods confirmed the predominance of power and communication systems in anomaly detection, with additional context from flight dynamics and computational load.


FNN: SHAP Summary Plot (Class: 1)
Used_RAM_MB
global_position-local_pose.pose.position.x
CPU_Percent
global_position-raw-satellites_data
state_guided
global_position-local_pose.pose.position.y
setpoint_raw-target_global_altitude
imu-data_orientation.w
global_position-local_pose.pose.position.z
global_position-global_altitude
global_position-local_pose.pose.orientation.x
vfr_hud_groundspeed
global_position-global_longitude
battery_voltage
rc-out_channels_3
vfr_hud_altitude
global_position-local_pose.pose.orientation.z
setpoint_raw-global_altitude
setpoint_raw-global_latitude
vfr_hud_throttle
−0.2
0.0
0.2
0.4
0.6
High
Low
Feature value




| Feature | Value |
|---|---|
| Used_RAM_MB | -0.69 |
| setpoint_raw-global_latitude | -0.88 |
| RSSI_Signal | 0.88 |
| setpoint_raw-target_global_longitude | -0.84 |
| setpoint_raw-global_longitude | -0.84 |
| imu-data_orientation.x | -0.23 |
| imu-data_angular_velocity.z | -1.68 |
| rc-out_channels_1 | -0.39 |
| setpoint_raw-global_altitude | 1.30 |
| global_position-local_twist.twist.linear.y | -1.39 |

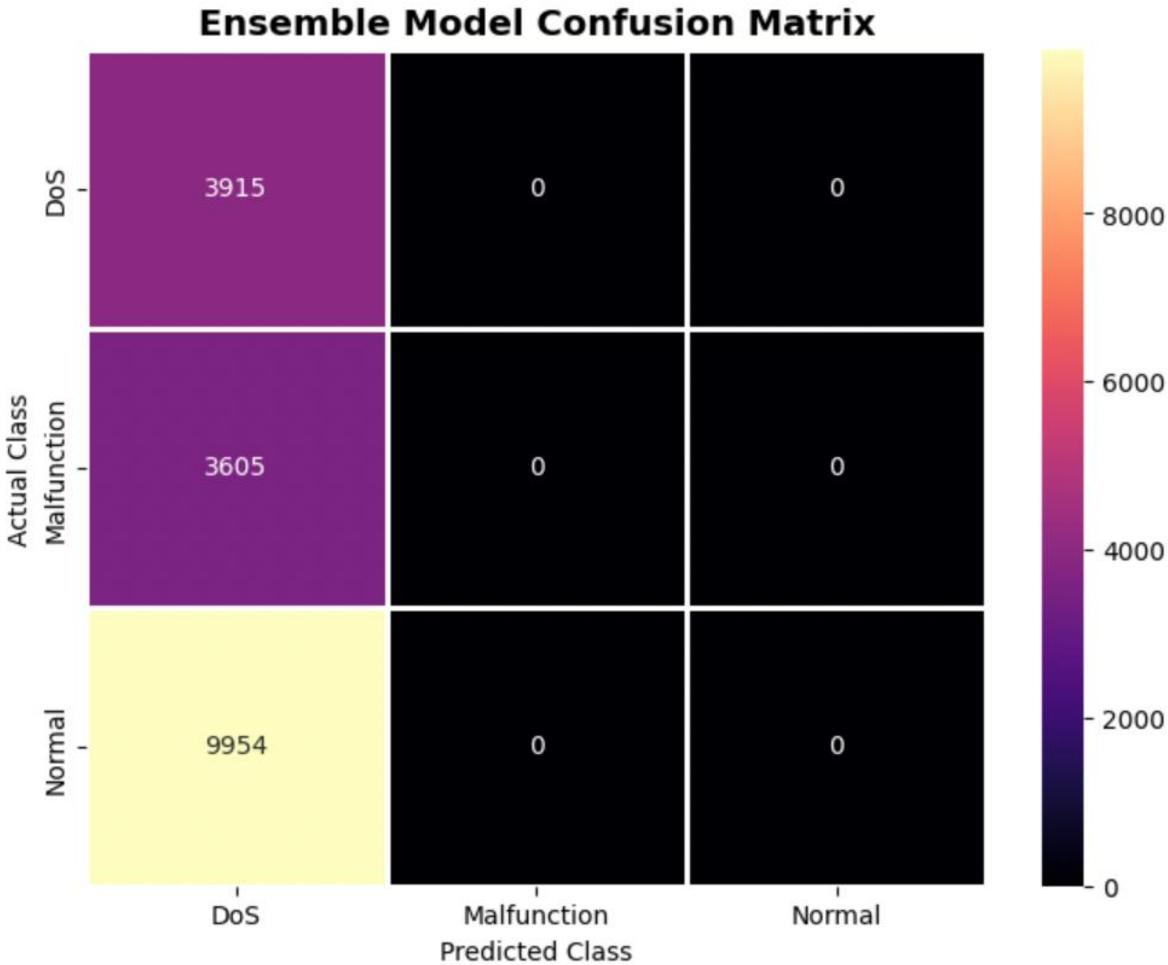
| Feature | Value |
|---|---|
| Used_RAM_MB | -0.69 |
| global_position-local_pose.pose.position.x | 1.95 |
| global_position-local_pose.pose.position.y | -1.64 |
| global_position-local_pose.pose.position.z | 1.48 |
| imu-data_orientation.w | 1.63 |
| battery_voltage | 1.09 |
| CPU_Percent | -0.39 |
| setpoint_raw-global_altitude | 1.30 |
| vfr_hud_throttle | 0.37 |
| setpoint_raw-global_latitude | -0.88 |

## 6.4. Partial Dependence Patterns

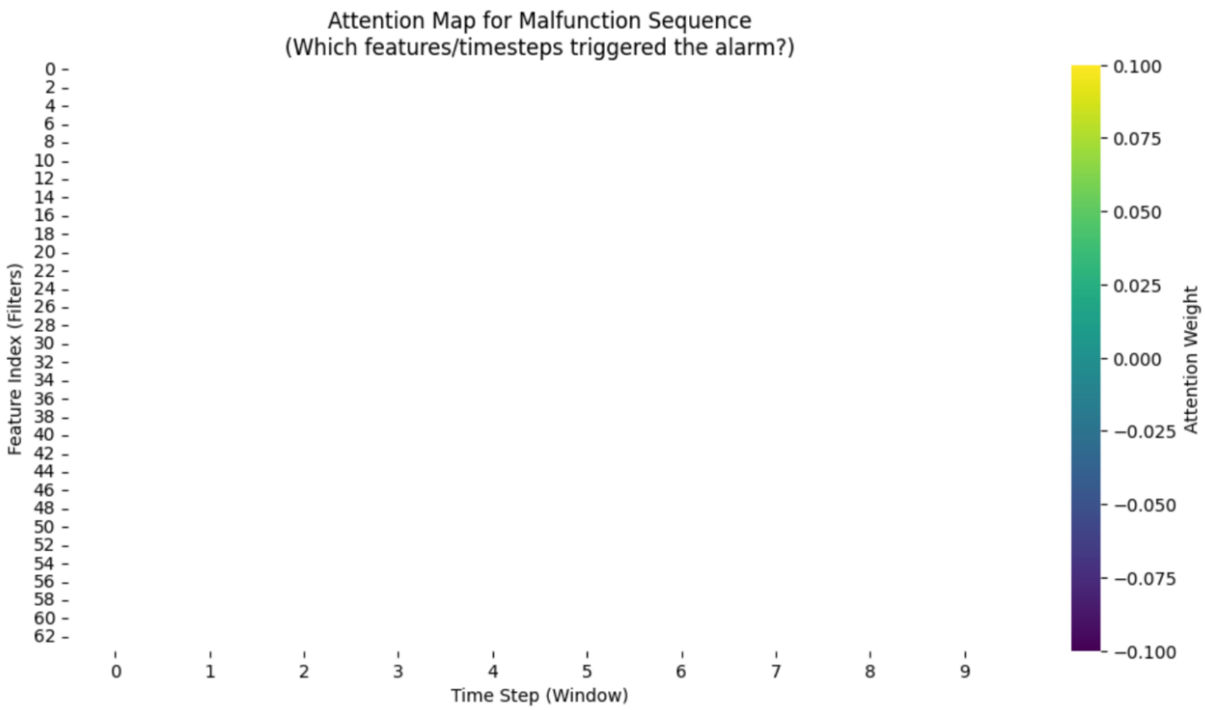
Non-linear relationships dominated the feature-target mappings, with clear operational boundaries between normal and anomalous states. Compounding effects were observed when multiple systems operated near their operational limits simultaneously.

## 6.5. Temporal Attention Analysis

For sequential models, attention mechanisms revealed characteristic focusing patterns: distributed attention during normal operation, concentrated attention during communication disruptions, and erratic attention during mechanical failures.



Ensemble Model Confusion Matrix
DoS
Malfunction
Normal
Actual Class
3915
0
0
3605
0
0
9954
0
0
DoS
Malfunction
Normal
Predicted Class
8000
6000
4000
2000
0


Attention Map for Malfunction Sequence
(Which features/timesteps triggered the alarm?)
Feature Index (Filters)
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
42
44
46
48
50
52
54
56
58
60
62
0
1
2
3
4
5
6
7
8
9
Time Step (Window)
0.100
0.075
0.050
0.025
0.000
−0.025
−0.050
−0.075
−0.100
Attention Weight

# 7. Conclusions & Recommendations

The analysis demonstrates that machine learning can effectively classify UAV operational states while providing interpretable decision insights. Tree-based models offer the optimal balance for deployment, combining strong predictive performance with computational efficiency and inherent interpretability. Feature importance analysis consistently identifies power systems, computational resources, and communication integrity as primary indicators of operational health.