



An AI-Driven Intrusion Detection System to Defend Against Satellite Hijacking

Karunathilake K. K. H.

Reg. No.: MS24014922

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

December 2025

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Mr. Kavinga Yapa Abeywardena

Approved for MSc Research Project:



MSc in IT Program Coordinator, SLIIT

Approved for MSc:

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Signature: 

Karunathilake K. K. H.

Date: 01.11.2025

ABSTRACT

An AI- Driven Intrusion Detection System to Defend Against Satellite Hijacking

Himashi Karunathilake

MSc in Information Technology

Supervisor: Mr. Kavinga Yapa Abeywardena

December 2025

The increasing reliance of the world on satellite systems has made them prime targets for cyber threats, with satellite orbital manipulation, a form of satellite hijacking, posing a critical national security risk due to its potential for disrupting essential infrastructure. To address this threat, this research proposes a novel Artificial Intelligence (AI)-based anomaly detection system tailored for identifying suspicious orbital maneuvers. The study employs Machine Learning (ML) models to analyze a custom dataset derived from the public European Space Agency Anomaly Detection Benchmark (ESA-ADB). This dataset was rigorously pre-filtered to include only anomalies occurring within a ± 48.00 hours window of a telecommand execution, thereby creating a naturally balanced, command-linked dataset to proxy for the kinematic footprint of a cyberattack. Findings established that temporal pattern recognition is paramount for detecting these attacks. LSTM networks emerged as the most promising model, leveraging their ability to learn sequential dependencies to achieve a high recall rate of 95.64% with a corresponding precision of 90.88%. Furthermore, a novel physics validation gate, grounded in orbital mechanics, was incorporated as a final, non-negotiable security layer. This component is vital, as it confirms that detected anomalies are physically non-nominal deviations, transforming raw statistical alerts into high-confidence cybersecurity indicators and dramatically boosting the overall trustworthiness and suitability of the system for operational deployment.

ACKNOWLEDGEMENT

I might not have been able to successfully conclude this yearlong research, if not for the immeasurable encouragement, guidance, support, and contribution of the many individuals behind the curtains.

Firstly, I would like to thank my Supervisor, Mr. Kavinga Yapa Abeywardena for his immeasurable guidance and support in conducting this research. The knowledge and the experience he shared, undoubtedly paved way for me to successfully complete this research. I would also like to thank Dr. Sara Vecchini, who provided technical supervision for this research, for always pointing me in the correct direction and sharing her knowledge and expertise.

I am also thankful to Mr. Prasanna Shankar who is a part of the Ansys / Synopsys Academic Program Team for his support in obtaining the required licensing for Ansys Systems Tools Kit (STK), which was extremely beneficial for my research.

I would also like to extend my sincere gratitude to all my lecturers and my research panel members for the immense knowledge they shared with me during the course of these past two years, which undoubtedly helped me to achieve my objectives for this research.

I also want to thank my friends for always sharing their feedback and experience with me.

Finally, my utmost gratitude goes out to my parents and my brother, who were there with me since the beginning, supporting me in my journey.

Table of Contents

DECLARATION	ii
ABSTRACT.....	iii
ACKNOWLEDGEMENT	iv
Table of Contents.....	v
List of Figures	viii
List of Tables	xi
List of Abbreviations	xiii
Chapter 1 Introduction.....	1
1.1 Background.....	1
1.2 Research Problem	5
1.3 Objectives	9
Chapter 2 Literature Review.....	10
2.1 Review of Existing Literature.....	10
2.2 Gap Identification	19
2.3 Significance of the Study	20
2.4 Expected Contributions.....	21
Chapter 3 Research Objectives.....	23
3.1 Main Research Objective.....	23
3.2 Hypotheses.....	23
3.3 Research Questions and Specific Research Objectives	24
Chapter 4 Research Design and Methodology	26
4.1 Research Design.....	26
4.2 Sampling Strategy.....	26
4.3 Research Methodology	27
4.3.1 Data Collection and Acquisition.....	29

4.3.2	Data Analysis	32
4.3.3	Data Preprocessing and Cleaning	33
4.3.4	Feature Engineering and Selection	33
4.3.5	Data Splitting and Validation Strategy	34
4.3.6	Data Balancing and Sampling.....	34
4.3.7	Feature Scaling and Normalization.....	35
4.3.8	Model Development and Architecture Design	35
4.3.9	Training and Optimization	35
4.3.10	Evaluation and Validation.....	36
4.3.11	Visualization and Interpretation.....	36
4.3.12	Model Persistence	37
Chapter 5	Implementation and Testing	38
5.1	Implementation of Various Models	38
5.1.1	Random Forest	38
5.1.2	XGBoost	42
5.1.3	Long Short-Term Memory.....	46
5.1.4	Autoencoders	50
5.2	Physics Validation	56
5.2.1	Orbital Mechanics	56
5.2.2	Ground Truth Data Generation	61
5.2.3	Implementation of the Physics Validation Gate	65
5.3	Performance Evaluation Metrics.....	66
5.3.1	Accuracy	67
5.3.2	Precision.....	68
5.3.3	Recall	68
5.3.4	F1-Score.....	69
5.3.5	True Positive Rate.....	69

5.3.6	True Negative Rate	70
5.3.7	False Positive Rate	70
5.3.8	False Negative Rate	71
Chapter 6	Results and Discussion	72
6.1	Model Performance.....	72
6.1.1	Random Forest Models	72
6.1.2	XGBoost Models	83
6.1.3	Long Short-Term Memory Models.....	96
6.1.4	Autoencoder Models.....	109
6.1.5	Evaluation of Anomaly Detection in All Models	123
6.2	Physics Validation Results.....	126
6.2.1	Importance of Physics Validation for Cybersecurity.....	126
6.2.2	Physics Validation Results.....	127
6.2.3	Evaluation of Physics Validation Results of All Models.....	138
Chapter 7	Limitations	140
Chapter 8	Future Research	142
Chapter 9	Ethical Considerations	143
9.1	Mitigation of Bias	143
9.2	Responsible Use of Publicly Available Telemetry Data.....	144
9.2.1	Acknowledgement of Data Sensitivity	144
9.2.2	Respect for Data Ownership and Purpose	145
9.2.3	Transparency and Reproducibility	145
9.2.4	Avoiding Misuse of Findings.....	145
Chapter 10	Conclusion	147
Chapter 11	References.....	148

List of Figures

Figure 1.1 Components of a satellite communication system	2
Figure 1.2 Space image by the team mHACKeroni for Hack-A-Sat 4 [8]	3
Figure 1.3 Space image by the team Krautsat for Hack-A-Sat 4 [8]	3
Figure 1.4 Space image by the team Poland Can Into Space for Hack-A-Sat 4 [8]	4
Figure 1.5 Graphical representation of the findings by Willbold et al. [13]	6
Figure 1.6 Comparison between 2012 and 2022 top 5 risks to satellites [14]	7
Figure 1.7 Comparison of the 2012 and 2022 likelihood of intercepting data [14]	8
Figure 1.8 Comparison of the 2012 and 2022 likelihood of satellite hijacking [14]	8
Figure 2.1 Process for anomaly prediction as proposed by Habib et al. [22]	13
Figure 4.1 Physics-informed anomaly detection pipeline	28
Figure 4.2 Cross validation between traditional security measures and the proposed approach	29
Figure 4.3 Structure of the ESA-ADB dataset	33
Figure 5.1 Orbit configuration for ground truth generation	64
Figure 5.2 Force model gravity configuration for ground truth generation	64
Figure 5.3 Force model atmospheric drag configuration for ground truth generation	64
Figure 5.4 Force model solar radiation pressure configuration for ground truth generation	65
Figure 5.5 Workflow of the physics validation gate	66
Figure 6.1 Comparison of overall performance metrics of the Random Forest models	73
Figure 6.2 Target recall vs. actual recall for Random Forest models	73
Figure 6.3 Target precision vs. actual precision for Random Forest models	74
Figure 6.4 Target F1-Score vs. actual F1-Score for Random Forest models	74
Figure 6.5 Target accuracy vs. actual accuracy for Random Forest models	75
Figure 6.6 Comparison of the diagnostic metrics of the Random Forest models	76
Figure 6.7 Target TPR vs. actual TPR for Random Forest models	76
Figure 6.8 Target TNR vs. actual TNR for Random Forest models	77
Figure 6.9 Target FPR vs. actual FPR for Random Forest models	77
Figure 6.10 Target FNR vs. actual FNR for Random Forest models	78

Figure 6.11 Confusion matrix of the Random Forest baseline model	79
Figure 6.12 PR curves for the Random Forest baseline model.....	80
Figure 6.13 Confusion matrix of the Random Forest high recall focused model.....	80
Figure 6.14 PR curves for the Random Forest high recall focused model	81
Figure 6.15 Confusion matrix of the Random Forest balanced precision-recall model	82
Figure 6.16 PR curves for the Random Forest balanced precision-recall model.....	83
Figure 6.17 Comparison of overall performance metrics of the XGBoost models	84
Figure 6.18 Target recall vs. actual recall for XGBoost models	84
Figure 6.19 Target precision vs. actual precision for XGBoost models.....	85
Figure 6.20 Target F1-Score vs. actual F1-Score for XGBoost models.....	85
Figure 6.21 Target accuracy vs. actual accuracy for XGBoost models.....	86
Figure 6.22 Comparison of the diagnostic metrics of the XGBoost models	87
Figure 6.23 Target TPR vs. actual TPR for XGBoost models.....	87
Figure 6.24 Target TNR vs. actual TNR for XGBoost models	88
Figure 6.25 Target FPR vs. actual FPR for XGBoost models	88
Figure 6.26 Target FNR vs. actual FNR for XGBoost models.....	89
Figure 6.27 Confusion matrix for the XGBoost baseline model	90
Figure 6.28 PR curves for the XGBoost baseline model.....	91
Figure 6.29 Confusion matrix for the XGBoost high recall focused model.....	92
Figure 6.30 PR curves for the XGBoost high recall focused model.....	93
Figure 6.31 Confusion matrix for the XGBoost balanced precision-recall model	94
Figure 6.32 PR curves for the XGBoost balanced precision-recall model	95
Figure 6.33 Random Forest and XGBoost best model comparison.....	95
Figure 6.34 Comparison of overall performance metrics of the LSTM models.....	97
Figure 6.35 Target recall vs. actual recall for LSTM models	97
Figure 6.36 Target precision vs. actual precision for LSTM models	98
Figure 6.37 Target F1-Score vs. actual F1-Score for LSTM models	98
Figure 6.38 Target accuracy vs. actual accuracy for LSTM models	99
Figure 6.39 Comparison of the diagnostic metrics of the LSTM models.....	100
Figure 6.40 Target TPR vs. actual TPR for LSTM models	100
Figure 6.41 Target TNR vs. actual TNR for LSTM models.....	101
Figure 6.42 Target FPR vs. actual FPR for LSTM models	101
Figure 6.43 Target FNR vs. actual FNR for LSTM models	102

Figure 6.44 Confusion matrix for the LSTM baseline model.....	103
Figure 6.45 PR curves for the LSTM baseline model	104
Figure 6.46 Confusion matrix for the LSTM high recall focused model	104
Figure 6.47 PR curves for the LSTM high recall focused model	105
Figure 6.48 Confusion matrix for the LSTM balanced precision-recall model.....	106
Figure 6.49 PR curves for the LSTM balanced precision recall model.....	107
Figure 6.50 Random Forest and LSTM best model comparison	108
Figure 6.51 XGBoost and LSTM best model comparison	108
Figure 6.52 Comparison of overall performance metrics of the Autoencoder models	110
Figure 6.53 Target recall vs. actual recall for Autoencoder models.....	110
Figure 6.54 Target precision vs. actual precision for Autoencoder models	111
Figure 6.55 Target F1-Score vs. actual F1-Score for Autoencoder models	111
Figure 6.56 Target accuracy vs. actual accuracy for Autoencoder models	112
Figure 6.57 Comparison of the diagnostic metrics of the Autoencoder models.....	113
Figure 6.58 Target TPR vs. actual TPR for Autoencoder models	113
Figure 6.59 Target TNR vs. actual TNR for Autoencoder models.....	114
Figure 6.60 Target FPR vs. actual FPR for Autoencoder models	114
Figure 6.61 Target FNR vs. Actual FNR for Autoencoder models	115
Figure 6.62 Confusion matrix for the Autoencoder baseline model.....	116
Figure 6.63 PR curves for the Autoencoder baseline model	117
Figure 6.64 Confusion matrix for the Autoencoder VAE model	118
Figure 6.65 PR curves for the Autoencoder VAE model	119
Figure 6.66 Confusion matrix for the advanced preprocessing model	120
Figure 6.67 PR curves for the Autoencoder advanced preprocessing model	121
Figure 6.68 Random Forest and Autoencoder best model comparison	121
Figure 6.69 XGBoost and Autoencoder best model comparison	122
Figure 6.70 LSTM and Autoencoder best model comparison.....	123
Figure 6.71 Random Forest, XGBoost, LSTM, and Autoencoder best model comparison.....	124
Figure 6.72 Target precision vs. improved precision for all best performing models	139

List of Tables

Table 5.1 Comparison of the preprocessing strategies of the Random Forest models	41
Table 5.2 Comparison of the model architectures of the Random Forest models	41
Table 5.3 Comparison of the thresholds used to train each Random Forest model.....	42
Table 5.4 Time taken to train each Random Forest model	42
Table 5.5 Comparison of the regularization strategy of the XGBoost models	45
Table 5.6 Comparison of the thresholds used to train each XGBoost model	46
Table 5.7 Time taken to train each XGBoost model	46
Table 5.8 Comparison of the feature dimensionality strategy of the LSTM models...	49
Table 5.9 Model complexity evolution of the LSTM models	49
Table 5.10 Comparison of the thresholds used to train each LSTM model	50
Table 5.11 Comparison of the thresholds used to train each LSTM model	50
Table 5.12 Evolution of the Autoencoder feature engineering strategy	55
Table 5.13 Comparison of the thresholds used to train each Autoencoder model	56
Table 5.14 Comparison of the thresholds used to train each Autoencoder model	56
Table 5.15 Summary of the model evaluation metrics	71
Table 6.1 Comparison of overall performance metrics of the Random Forest models	72
Table 6.2 Comparison of the diagnostic metrics of the Random Forest models	75
Table 6.3 Comparison of overall performance metrics of the XGBoost models.....	83
Table 6.4 Comparison of the diagnostic metrics of the XGBoost models.....	86
Table 6.5 Comparison of overall performance metrics of the LSTM models	96
Table 6.6 Comparison of the diagnostic metrics of the LSTM models	99
Table 6.7 Comparison of overall performance metrics of the Autoencoder models .	109
Table 6.8 Comparison of the diagnostic metrics of the Autoencoder models	112
Table 6.9 Best-performing models from each family, ranked by recall	124
Table 6.10 Best-performing models from each family, ranked by precision	124
Table 6.11 Best-performing models from each family, ranked by F1-Score	124
Table 6.12 Best-performing models from each family, ranked by accuracy	125
Table 6.13 Physics validation results of the baseline Random Forest model.....	128
Table 6.14 Physics validation results of the high recall focused Random Forest model	129

Table 6.15 Physics validation results of the balanced precision-recall Random Forest model.....	130
Table 6.16 Physics validation results of the baseline XGBoost model	131
Table 6.17 Physics validation results of the high recall focused XGBoost model....	131
Table 6.18 Physics validation results of the balanced precision-recall XGBoost model	132
Table 6.19 Physics validation results of the baseline LSTM model.....	133
Table 6.20 Physics validation results of the high recall focused LSTM model	134
Table 6.21 Physics validation results of the balanced precision-recall LSTM model	135
Table 6.22 Physics validation results of the baseline Autoencoder model.....	136
Table 6.23 Physics validation results of the VAE Autoencoder model.....	136
Table 6.24 Physics validation results of the advanced preprocessing Autoencoder model.....	137
Table 6.25 Best-performing models from each family, ranked by improved precision	139

List of Abbreviations

Abbreviation	Definition
1DCNN	One-Dimensional Convolutional Neural Network
3D	Three Dimensional
ADAPT-Lite	Advanced Diagnostics And Prognostics Testbed-Lite
AI	Artificial Intelligence
ALFA	Air Laboratory Failure and Anomaly
ARIMA	Auto Regressive Integrated Moving Average
ASAT	Anti-Satellite
AUC	Area Under the Curve
BADMM	Bregman Alternating Direction Method of Multipliers
CAE	Convolutional Autoencoder
CEG	Causality Enhanced Graph
cFS	core Flight System
CPS	Cyber Physical System
CTF	Capture the Flag
DCDSPOT	Double-Criteria Drift Streaming Peaks Over Threshold
DDMN	Deviation Divide Mean over Neighbors
DDTS	Dynamic Detection Threshold Setting
DTW	Dynamic Time Warping
Ecc	Eccentricity
EPS	Electrical Power System
ESA	European Space Agency
ESA-ADB	European Space Agency Anomaly Detection Benchmark

F1PA	F1 Point Adjust
FastICA	Fast Independent Component Analysis
FC	F1-Score Composite
FCC	Flight Control Center
FNR	False Negative Rate
FPR	False Positive Rate
GA	Genetic Algorithm
GCC	Ground Control Center
GNN	Graph Neural Network
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRU	Gated Recurrent Unit
HPOP	High Precision Orbit Propagator
IDS	Intrusion Detection System
IF-CBLOF	Isolation Forest and Clustering-Based Local Outlier Factor
Inc	Inclination
IQR	Inter-Quartile Range
K-DTWAN	K-Dynamic Time Wrapping Distance Adjacent Nodes
K-SVD	K-Means Singular Value Decomposition
KNN	K-Nearest Neighbors
KDE	Kernel Density Estimation
KL	Kullback-Leibler
LEO	Low Earth Orbit
LIME	Local Interpretable Model-Agnostic Explanations
LRP	Layer-wise Relevance Propagation
LSTM	Long Short-Term Memory
MCDA	Multi-Criteria Decision Analysis
ML	Machine Learning

MSE	Mean Squared Error
MSL	Mars Science Laboratory
MTAD	Multi-Task Anomaly Detection
NASA	National Aeronautics and Space Administration
NB65	Network Battalion 65
OBCS	On-Board Computer System
OCKELM	One-Class Kernel Extreme Learning Machine
OCSVM	One-Class Support Vector Machine
OOL	Out-Of-Limit
PCA	Principal Component Analysis
PR	Precision-Recall
QPSO	Quantum-behaved Particle Swarm Optimization
RaaS	Ransomware-as-a-Service
RNN	Recurrent Neural Network
ROSCOSMOS	Russian State Corporation for Space Activities
RPM	Revolutions Per Minute
RWL	Reaction Wheels
SACS	Satellite Attitude and Control System
SFAD	Sparse Feature-based Anomaly Detection
SHAP	Shapley Addictive Explanations
SJ-21	Shijian-21
SMA	Semi-Major Axis
SMAP	Soil Moisture Active Passive
SSO	Sun-Synchronous Orbit
STCG	Spatial-Temporal Causal Graph
STK	Systems Tool Kit
SVDD	Support Vector Data Description
TGAK	Triangular Global Alignment Kernel

TGAK-OCELM	Triangular Global Alignment Kernel One-Class Extreme Learning Machine
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate
UAV	Unmanned Aerial Vehicle
VAE	Variational Autoencoder