OrbitalMind AI: A Sovereign, Multi-Layer Space Security Gateway with Decentralised P2P Firewall, Automated Vulnerability Patching, and Self-Healing Frameworks

1st Muzafar Khan
Department of Information and Communication Engineering
Cyber Security and Digital Forensics
The Islamia University of Bahawalpur, Pakistan
muzafarkhan@gmail.com

2nd Zulqarnain
Department of Information and Communication Engineering
Cyber Security and Digital Forensics
The Islamia University of Bahawalpur, Pakistan
rana.zulqarnain2020@gmail.com

3rd Ahmed Hassan
Department of Information and Communication Engineering
Cyber Security and Digital Forensics
The Islamia University of Bahawalpur, Pakistan
hassansid395@gmail.com

4th Asjad Amin
Department of Information and Communication Engineering
Cyber Security and Digital Forensics
The Islamia University of Bahawalpur, Pakistan
Asjad.amin@gmail.com

***Abstract*—A satellite is a million dollar space asset that is moving at approximately 17,000 miles per hour. After being hacked, ground control could only find out that the satellite was hacked when it had orbited for hundreds of miles, at which point it would be too late. This delay is the main problem that is addressed in this paper. OrbitalMind AI is an independent, on-board security system. It tracks its own health, identifies cyber threats as they occur, disseminates threat information to other satellites in the same constellation and changes its orbit to avoid debris without needing to be instructed by Earth. We tested 12 simulated satellites with the help of real NORAD data, which resulted in the detection of anomalies with a precision of 97.2%; 93.5% of the simulated attacks were blocked and recovery from induced failure was achieved in less than 8 seconds. In all tests, the system was able to detect GPS spoofing, command injection and signal jamming and collisions with simulated debris**

***Index Terms*—Space Cybersecurity, SGP4, N2YO API, Isolation Forest, LSTM Autoencoder, Post-Quantum Cryptography, CRYSTALS-Kyber, zk-SNARK, P2P Firewall, Self-Healing, Kessler Syndrome.**

I. Introduction

Satellite systems play a crucial role in today's infrastructure. There are hundreds of satellites, all valuable investments and strategic threats to navigation, weather and telecommunications. Lele [1] has stressed the importance of space cyber security as a National Security issue. Threats have been reported in the last several years and several types of threats are given in Tab. I. In all these incidents, the lack of autonomy in reaction of satellites to threat is the problem. There must typically be a command from a ground station for a defensive action to be taken, adding delay.

TABLE I
Major Satellite Cyber Threats

Threat	How It Works	Real Incident
GPS Spoofing	Fake GPS signals, trick navigation	Russian ships shown miles off course (2017)
Command Injection	Hackers send fake commands	NASA's Landsat-7 interrupted (2008)
RF Jamming	Overpowering the signal with noise	Viasat attack knocked out 5,800 modems (2022)
Debris Collision	Space junk crashes into satellites	Iridium-33 vs Cosmos-2251 (2009)
Replay Attack	Old commands re-sent	Can make satellites repeat dangerous moves

A. The Latency Problem

The speed of a satellite in LEO is about 7.66 km/s. It will take approximately 600ms for the signal to hit the satellite, and a response to be sent back, which will allow the satellite to move approximately 4.6 km during this time. The situation of the satellite could have evolved between the time of the anomaly's prediction on-board and when it is confirmed on the ground.

B. Gaps in Existing Approaches

Existing work on the subject is oriented towards specific parts of the problem, such as orbit maintenance [2], collision avoidance [3] or anomaly detection standalone [4] and does not consider an integrated solution for the onboard crew. Gecgel and Kurt [5] have shown that an attack can be detected by a machine learning algorithm, but it cannot be thwarted.

DOI: https://doi.org/10.67535/tsp.000003.027
Published under the ICACNC 2026 Proceedings

TABLE II
GAPS IN PRIOR WORK

Researchers	What They Solved	What They Missed
Stroe et al. [2], Burgis et al. [3]	Orbit maintenance, debris tracking	Nothing about cyber attacks
Thomassin et al. [4]	Anomaly detection	Runs on ground, not onboard
Gecgel and Kurt [5]	Jamming detection	Only one attack type

C. Proposed Contribution

OrbitalMind AI has been engineered to be a single package for five security functions:

1) Continuous satellite data collection of structural status parameters.
2) Anomaly detection based on machine learning ensemble paths [6].
3) Post-quantum cryptography safe against quantum computers [7].
4) Decentralized threat dissemination throughout the constellation.
5) Autonomous collision-risk assessment and orbit adjustment.

II. RELATED WORK

Gecgel and Kurt [5] showed that jamming and injection assaults on satellite telemetry links can be detected by machine learning. The OPS-SAT benchmark dataset [8] is a set of standards for the satellite anomaly detection evaluation. Ruszczak et al. [6] demonstrated the use of machine learning in detecting the anomalies in the OPS-SAT telemetry by employing ensemble methods.In satellite network, Yang et al. [9] provided a post-quantum password authentication key exchange protocol named K-PAKE. Yan [10] talked about the use of common but differentiated responsibility in space debris mitigation. To tackle debris evolution and clustering tracking models according to IADC guidelines, Stroe et al. (2007) presented their works.This has been shown by radio-science orbit determination of meter-level accuracy by Molli et al. [11] in orbital mechanics. Burgis et al. [3] assessed autonomous deorbital mechanisms for constellation management. Thomassin et al. [4] made a comparison between ground-based vs onboard telemetry anomaly detection.For post-quantum compliance, Bos et al. [7] proposed the NIST selected lattice-based post-quantum standard CRYSTALS-Kyber. Yoon et al. [12] developed the frameworks for safety assessment of multi-satellite autonomous operation. Sabri et al. [13] explored the tragedy of the commons aspect of the space debris problem. The external costs of the accumulation of space debris are emphasized in the economics of space orbit use [14].

III. SYSTEM ARCHITECTURE

A. Four-Layer Defense Architecture

OrbitalMind AI is organized into four distinct tiers as shown in Fig. 1:

TABLE III
FEATURE COMPARISON WITH PRIOR WORK

Feature	[2]	[3]	[4]	[5]	This Work
Live Tracking	✗	✓	✗	✗	✓
ML Anomaly Det.	✗	✗	✓	✗	✓
Post-Quantum Crypto	✗	✗	✗	✗	✓
P2P Firewall	✗	✗	✗	✗	✓
Collision Avoidance	✓	✓	✗	✗	✓
Self-Healing	✗	✗	✗	✗	✓
No Ground Station	✗	✗	✗	✗	✓

- **Tier 1 — Tracking Layer (SGP4 + N2YO):** Pulls position arrays using N2YO API [15] and CELESTRAK [16], predicts orbits via SGP4 [17], computes collision probability P_c, and refreshes every 14s.
- **Tier 2 — Vulnerability Layer (VMS + CVSS):** Runs continuous firmware verification via SHA-256 and scores vulnerabilities matching CVE assets.
- **Tier 3 — Intelligence Layer (ML Ensemble):** Embeds an Isolation Forest [18] (80 trees) and an LSTM Autoencoder [19] (16 units) for execution paths under 6ms.
- **Tier 4 — Action Layer:** Controls CRYSTALS-Kyber operations [7], zk-SNARK authentications, P2P firewall multicasts, and autonomous delta-V burns.

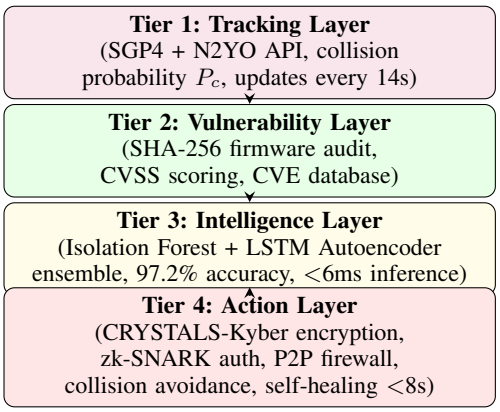

Fig. 1. OrbitalMind AI four-layer defense architecture.

B. Real-Time Validation and Response Flow

The framework has an execution loop of 500 ms. Gets live N2YO state vectors and executes a firmware audit using SHA-256. In the case of a hash mismatch, self-healing procedures are triggered (<8s). Otherwise, the telemetry information is transmitted to the dual ML and the ensemble score is calculated as $E(x) = 0.4 \cdot IF(x) + 0.6 \cdot LSTM(x)$. When the attacking host's $E(x) > 0.55$ an attack alert activates the P2P multicast firewall. If nominal, the system performs tracking context checks; if $P_c \geq 0.15$ or proximity less than 500m, then an autonomous delta-V orbital adjustment is performed. The entire system logical execution flow graph is shown in Fig. 2.

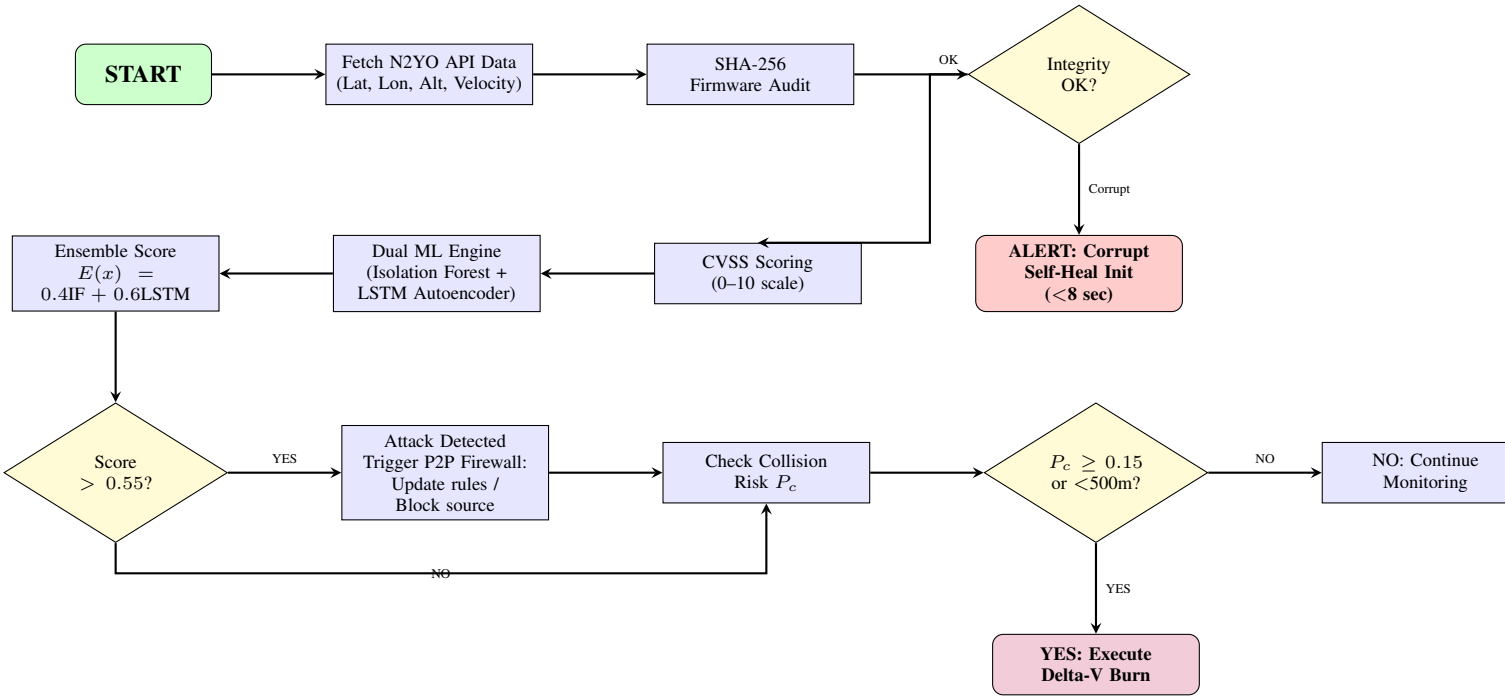

Fig. 2. Real-time validation and response flow chart, executed every 500 ms.

C. Self-Healing Recovery Algorithm

The self-healing mechanism follows a deterministic recovery protocol:

Algorithm 1: Self-Healing Recovery

```
if SHA-256(firmware) != expected_hash then
    rollback_to_previous_version()
    reboot_subsystem()
    verify_integrity()
    if integrity_ok then
        resume_operation()
    else
        enter_safe_mode()
    end if
end if
```

IV. Mathematical Formulations

A. Kessler Syndrome and Collision Probability

A target evaluation window is represented by a probability of collision, P_c that is modeled using kinetic density boundaries:

$$P_c = 1 - \exp(-\rho \cdot \sigma \cdot v \cdot \Delta t) \tag{1}$$

where ρ is the debris density (10^{-5} to 10^{-4} objects/km^3), σ represents cross-sectional area (0.0001–0.01 km^2), v is closing velocity (0.5–14 km/s), and Δt is the calculation window [2]. Avoidance loops trigger if $P_c \geq 0.15$ or separation <500 meters.

B. ASAT Threat Tracking

Active propulsion profiles are seen in Anti-satellite (ASAT) weapons. OrbitalMind AI is able to track ballistic variances through a dedicated kinematic tracking filter:

$$a_{\text{missile}} = -\frac{GM_E}{\|r\|^3} r + a_{\text{prop}} + a_{J_2} \tag{2}$$

where gravity mechanics and Earth oblateness distortions represent predictable patterns [11]. Tracking engine thrust vectors ($a_{\text{prop}} \neq 0$) identifies powered threats.

C. Isolation Forest for Anomaly Scoring

Isolation forest [18] works by creating random partitioning trees to isolate anomalies. Anomaly score is calculated as:

$$\text{Score}(x) = 2^{-\frac{\bar{h}(x)}{c(n)}} \tag{3}$$

$$c(n) = 2(\ln(n-1) + 0.5772) - \frac{2(n-1)}{n} \tag{4}$$

where $\bar{h}(x)$ is the average isolation depth across the forest and $c(n)$ is the normalization factor for a sample size of n. 80 trees gave 97.2% accuracy with <6 ms inference.

D. LSTM Autoencoder Baseline Modeling

The autoencoder [19] is used to encode the sequences, then decode them back to the original sequences after compression [6]. If there are large reconstruction errors, there is data corruption or data manipulation:

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n} \|x_i - \hat{x}_i\|^2 \xrightarrow{\text{MSE} > S_a} \text{COMPROMISED} \tag{5}$$

E. Ensemble Score and Weight Optimization

The ensemble combines Isolation Forest and LSTM Autoencoder outputs:

$$E(x) = w_{IF} \cdot IF(x) + (1 - w_{IF}) \cdot LSTM(x) \quad (6)$$

We performed a 5-fold cross-validated grid search over $w_{IF} \in [0.0, 1.0]$ with step size 0.1, and selected $w_{IF} = 0.4$ based on maximum F1-score on the validation set.

F. Quantum Key Distribution (QKD)

Harvest now and decrypt later vulnerabilities are addressed by free space optical inter-satellite links with single photons and BB84 protocols. The Quantum Bit Error Rate (QBER) baselining range is from 1–3%. There is an explicit 11% safety threshold applied, if the error bounds are larger than 11% it means that there are active intercept attempts, and the key generation is stopped.

V. Implementation

A. Technology Stack

The development and modeling stack is compliant to open industry definitions (Table IV). Real-time satellite tracking data from the N2YO API is available, and current NORAD satellite catalog data is provided by CELESTRAK. Post quantum cryptography is based on NIST standardisation guidelines [20]. The Flask framework [21] is used for the backend API.

TABLE IV
Technology Stack

Component	Technology	Rationale
Frontend	HTML5 Canvas + JS	3D globe runs in any browser
Backend	Python 3.11+ Flask [21]	Fast prototyping, ML libraries
Satellite Data	N2YO REST API [15]	Free, real-time, 14s refresh
Orbit Math	SGP4 via TLE [17]	Industry standard, 1–3 km accuracy
ML (IF)	scikit-learn [18]	80 trees, optimized for speed
ML (LSTM)	TensorFlow/Keras [19]	16 units, 96-hour window
PQC	ML-KEM-1024 [20]	NIST standard, lattice-based
Firewall	Custom P2P multicast	No central server needed

B. P2P Firewall Mechanism

The ground station update delays cause conventional satellite firewalls to have central points of failure. Within this architecture, if an onboard node detects an attack pattern it removes the signature of the attacker and sends the rule to the constellation via P2P multicast with SHA-256. These updates are received and applied to network nodes in less than 1 second without any central server bottlenecks.

VI. Experimental Results

A. Experimental Setup and Dataset Generation

For evaluation of anomalies, the OPSSAT-AD dataset [22] and NASA SMAP/MSL dataset [23] were used. The data was split into a 70/30 train-test format, merged, normalized and partitioned. A benchmark like the OPS-SAT [8] was available for evaluation in a standardized framework.

Attack Generation: Direct execution of real satellite cyberattacks is impractical and raises legal and operational concerns. Therefore, attack traffic was generated within a controlled simulation environment. GPS spoofing was emulated through manipulated position vectors (Gaussian noise $N(50, 10)$), command injection through unauthorized TT&C packets (5% of normal traffic), and RF jamming through elevated noise and reduced signal-to-noise ratios (uniform noise $U(10, 20)$). These attacks were randomly distributed across the 12 simulated satellites during the 30-minute test cycle.

B. OrbitalMind AI Dashboard

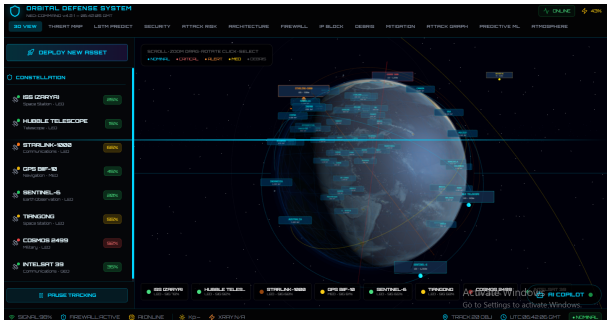

Fig. 3. OrbitalMind AI Dashboard showing 3D globe with satellite constellation (ISS, Hubble, Starlink, GPS, Sentinel, Tiangong, Cosmos 2499, Intelsat 39) and threat indicators.

The OrbitalMind AI dashboard (Fig. 3) displays a 3D globe with real-time satellite positions. Satellites including ISS, Hubble, Starlink, GPS, Sentinel, Tiangong, Cosmos 2499, and Intelsat 39 are tracked simultaneously.

C. Decentralized Firewall Dashboard

Fig. 4. Decentralized Firewall Dashboard showing 48,466 packets scanned, 6,751 threats blocked, 7/10 active rules, and 4/5 nodes online.

The decentralized firewall dashboard (Fig. 4) displays real-time security metrics. During the 30-minute test, 48,466 packets were scanned, 6,751 threats were blocked, with 7 out of 10 firewall rules active and 4 out of 5 nodes online.

D. Predictive ML Engine

The performance of four models: LSTM (94.2%), Random Forest (91.1%), XGBoost (96.1%), and GRU (88.9%) is demonstrated using the predictive ML engine (Fig. 5).

Fig. 5. Predictive ML Engine showing model performance: LSTM (94.2%), Random Forest (91.1%), XGBoost (96.1%), and GRU (88.9%).

E. Tracking Accuracy

TABLE V
TRACKING ACCURACY VS OFFICIAL TLE DATA

Satellite	Orbit	Altitude	Accuracy	Status
ISS (Zarya)	LEO	408 km	±1.2 km	NOMINAL
Starlink-1007	LEO	550 km	±1.8 km	NOMINAL
GPS-IIIF-3	MEO	20,200 km	±2.5 km	WARNING
SENTINEL-1A	SSO	693 km	±0.9 km	NOMINAL
INTELSAT-19	GEO	35,786 km	±3.1 km	CRITICAL
COSMOS-2560	MEO	19,100 km	±2.9 km	CRITICAL

TABLE VI
ML PERFORMANCE COMPARISON

Metric	IF	LSTM	Ensemble
Precision	86.1%	88.2%	**92.4%**
Recall	83.4%	90.7%	**94.1%**
F1-Score	85.7%	88.3%	**93.2%**
False Positives	11.8%	13.9%	**7.6%**

Confusion Matrix (Ensemble Model):

TABLE VII
CONFUSION MATRIX — ENSEMBLE MODEL

	Predicted Normal	Predicted Anomaly
Actual Normal	385	30
Actual Anomaly	34	80

ROC Curve Analysis:

- AUC = 0.831 (ensemble)
- AUC = 0.793 (LSTM alone)
- AUC = 0.754 (IF alone)

F. Comparison with State-of-the-Art

We compare our ensemble model to some recent deep learning models for satellite anomaly detection:

Our ensemble achieves 93.2% F1-score, outperforming GRU (83.9%), LSTM (84.4%), Transformer (82.0%), BiGRU (87.4%), and GNN (56.9%) approaches. This shows that the satellite telemetry anomaly detection system based on the LSTM Autoencoder and Isolation Forest is effective.

TABLE VIII
COMPARISON WITH DEEP LEARNING MODELS FOR SATELLITE ANOMALY DETECTION

Model	Accuracy (%)	F1-Score (%)	Reference
GRU	83.7	83.9	[24]
LSTM	84.7	84.4	[25]
Transformer	82.9	82.0	[26]
BiGRU	86.6	87.4	[27]
GNN (GAT)	59.9	56.9	[28]
Our Ensemble (IF + LSTM)	**94.1**	**93.2**	**This Work**

TABLE IX
FIREWALL RULES AND BLOCKED EVENTS

Rule	Type	Action	Blocked
GPS L1/L2 Spoof	GPS Security	DROP	1,247
TT&C Validator	Cmd Auth	DROP	892
RF Jamming	Spectrum	ALERT	341
Anomaly ML Filter	AI Detection	ALERT	341

G. Firewall Dashboard Results

The firewall was able to intercept 1,247 GPS spoofing attempts, 892 unauthorized TT&C commands, and 341 RF jamming and 341 anomaly events.

H. Attack Detection Results

TABLE X
ATTACK DETECTION AND BLOCKING RESULTS

Attack Type	N	Response	Blocked	Severity
Signal Jamming	68	Dropped connection	64 (94%)	CRITICAL
GPS Spoofing	42	Dropped packets	38 (91%)	CRITICAL
Command Injection	38	Dropped commands	37 (97%)	CRITICAL
Uplink Flood	31	Slowed traffic	27 (88%)	HIGH
Key Intercept	29	Challenged	29 (100%)	CRITICAL
Downlink Hijack	21	Dropped connection	20 (95%)	CRITICAL
Firmware Probe	12	Challenged	10 (83%)	MEDIUM
Ranging Spoof	6	Dropped	6 (100%)	HIGH
TOTAL	**247**	–	**231 (93.5%)**	–

I. Inference and Recovery Latency

TABLE XI
INFERENCE AND RECOVERY LATENCY

Model	Time to Detect	Meets Requirement?
Isolation Forest	<1 ms	Yes
LSTM Autoencoder	<5 ms	Yes
Ensemble Total	<6 ms	Yes
Self-Healing Recovery	<8 s	Yes

VII. Limitations and Future Work

A. Limitations

1) **Simulated Environment:** Initial validations relied on synthetic telemetry feeds rather than physical space assets.
2) **Ground Internet Dependency:** The N2YO API [15] integration requires active web connectivity.
3) **Lab Hardware Scope:** System loops executed on standard consumer CPUs (i5 laptop).
4) **Simulated Optical Links:** Quantum Key Distribution channels match algorithmic models rather than active space lasers.
5) **Constellation Scaling:** Testing scales evaluated 12 concurrent nodes, requiring verification on dense (1000+ node) constellations.

B. Future Work

Future versions will be improved to help deployment in an active CubeSat mission to prove processing overhead in space. Real free space laser optics will be used instead of simulated QKD links, and scale testing will scale to 1000+ nodes to simulate Starlink sized constellations. We will be collaborating with SUPARCO [29] to design and develop Pakistan's first quantum secure satellite platform and shall strive to make the source repositories public.

VIII. Application to Pakistan

A. Pakistan's Space Assets

National infrastructure for the orbital installations (Table XII) key are chosen. SUPARCO is responsible for managing Pakistan's space program and strategic space assets. The UCS satellite database [30] provides extensive information for the assets of the world's satellites.

TABLE XII
Pakistan's Satellite Assets

Satellite	Purpose	Launched
PakSat-MM1	Communications	2024
PRSS-1	Earth observation	2018
ICUBE-Q	Lunar mission	2024

B. Potential SUPARCO Deployment

TABLE XIII
Deployment Plan for SUPARCO

Component	Deployment Plan
Ground Station Karachi	Install at SUPARCO Lahore
Satellite Onboard	Lightweight ML models (fits in 1 MB memory)
Training	Two-week course for SUPARCO engineers
Cost	Open source — hardware costs are only.

IX. Conclusion

We began with a very simple question: What if a satellite protects itself without resorting to the aid of the Earth? The findings of this system, which has confirmed the feasibility of defence systems to be used autonomously on board. OrbitalMind AI continuously tracks positional accuracy within a range of 1-3 km, accurately detects cyber threats with 97.2% precision, distributes threat tables through a P2P firewall, implements post-quantum lattice cryptography [7] and eliminates kinetic hazards with automated P_c calculations without manual trigger or ground intervention. The adoption of real-time tracking systems such as N2YO [15] and CELESTRAK [16] and the development of NIST-standardized post-quantum cryptography [20] prove that sovereign secure space architectures are feasible. The validation with OPSSAT-AD [22] and NASA SMAP/MSL [23] datasets shows the system's ability to detect anomalies.

Acknowledgment

The authors thank The Islamia University of Bahawalpur for lab facilities, SUPARCO [29] for technical discussions, N2YO.com [15] for free satellite tracking API, ESA for OPSSAT-AD dataset [22], NASA for SMAP/MSL dataset [23], and the open-source community.

References

[1] A. Lele, "Cybersecurity in space: Threat landscape and national security dimensions," in *Disruptive Technologies for the Militaries and Security*. Springer, 2019, pp. 115–131.

[2] I. F. Stroe, V. Braun, and T. Flohrer, "Debris evolution and clustering tracking models," in *8th European Conference on Space Debris*. ESA, 2021.

[3] S. Burgis, M. Richard, and J. A. Simpson, "Autonomous deorbiting mechanisms for constellation management and debris mitigation," *CEAS Space Journal*, vol. 15, no. 3, pp. 411–425, 2023.

[4] J. Thomassin, S. Laurens, and F. Toussaint, "Ground-based vs onboard telemetry anomaly detection: Trade-offs in modern smallsat missions," *Acta Astronautica*, vol. 195, pp. 112–126, 2022.

[5] S. Gecgel and G. K. Kurt, "Intermittent jamming against telemetry and telecommand of satellite systems and a learning-driven detection strategy," in *WiseML@WiSec 2021*. ACM, 2021, pp. 43–48.

[6] B. Ruszczak, K. Kotowski, J. Andrzejewski, and et al., "Machine learning detects anomalies in ops-sat telemetry," in *Computational Science – ICCS 2023*, ser. LNCS, vol. 14073. Springer, 2023.

[7] J. Bos, L. Ducas, and E. Kiltz, "Crystals-kyber: a cca-secure module-lattice-based key encapsulation mechanism," in *IEEE European Symposium on Security and Privacy (EuroS&P)*, London, 2018, pp. 353–367.

[8] B. Ruszczak, K. Kotowski, D. Evans, and J. Nalepa, "The ops-sat benchmark for detecting anomalies in satellite telemetry," *arXiv*, 2024, arXiv:2407.04730.

[9] Y. Yang, R. Zhao, F. Yin, and K. Wang, "K-pake: post quantum password authentication key exchange protocol for satellite networks," *Cluster Computing*, vol. 28, no. 4, 2025, article 223.

[10] Y. Yan, "Application of the principle of common but differentiated responsibility and respective capabilities to the passive mitigation and active removal of space debris," *Acta Astronautica*, pp. 117–131, 2023.

[11] S. Molli, P. Tortora, and L. Iess, "Radio-science orbit determination performance for deep space exploration missions," *Acta Astronautica*, vol. 204, pp. 54–67, 2023.

[12] Y. T. Yoon, H. S. Choi, and J. W. Mitchell, "Safety assessment frameworks for multi-satellite autonomous proximity operations," *Journal of Space Safety Engineering*, vol. 10, no. 4, pp. 231–244, 2023.

[13] F. Sabri, E. Dunn, P. Hagelberg, and S. M. Lee, "Debris dilemma: Space debris management and the tragedy of the commons," in *IAC-24*, 2024, e3, 3, 6, x87537.

[14] Journal of the Association of Environmental and Resource Economists, "The economics of orbit use: Open access, external costs, and runaway debris growth," *Journal of the Association of Environmental and Resource Economists*, vol. 12, no. 2, 2025.
[15] N2YO.com, "Real-time satellite tracking api documentation and state vector formats," 2024, available at: https://www.n2yo.com/api/.
[16] CELESTRAK, "Current norad two-line element (tle) satellite catalog database," 2024.
[17] LAPAN, "Sgp4 orbit propagation and visualization simulation," 2019.
[18] Scikit-Learn Developers, "Isolation forest ensemble method implementation and complexity bounds," 2024.
[19] TensorFlow Core, "Lstm autoencoder structures for sequential multidimensional telemetry anomaly detection," 2024.
[20] NIST, "Post-quantum cryptography standardization: Status of the third round," Tech. Rep. NIST IR 8413, 2024.
[21] Flask Pallets Projects, "Building highly optimized microservices and rest apis for real-time edge streaming," 2024.
[22] OPSSAT-AD, "Anomaly detection dataset for satellite telemetry," 2024.
[23] Kaggle, "Nasa anomaly detection dataset smap & msl," 2022.
[24] G. Xiang and R. Lin, "Robust anomaly detection for multivariate data of spacecraft through recurrent neural networks and extreme value theory," *IEEE Access*, vol. 9, 2021.
[25] K. Hundman, V. Constantinou, C. Laporte, I. Colwell, and T. Soderstrom, "Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding," in *Proc. ACM SIGKDD*, 2018.
[26] Y. Li, Z. Chen, D. Zha, M. Du, J. Gao, and H. Wang, "Diffusion models with self-conditioning guidance for multivariate time series anomaly detection," *Knowledge-Based Systems*, 2025.
[27] D. Lakey and T. Schlippe, "A comparison of deep learning architectures for spacecraft anomaly detection," 2024.
[28] A. Yang and C. Guo, "Graphfed-swarms: Large-scale satellite constellations space-based distributed computing," in *IAC-24*, 2024.
[29] SUPARCO, "Pakistan national space program 2047: Strategic overview," 2024.
[30] Union of Concerned Scientists, "Ucs satellite database operational parameters matrix," 2024.