© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719027

Quantum-Resistant Homomorphic Encryption for Secure Federated Learning in CubeSat Constellations for Real-Time Exoplanet Detection

GOVIND MULCHANDANI
Indus International School Pune

Abstract- ***The growing adoption of CubeSat constellations has introduced a new era in exoplanetary science by enabling low-cost, distributed, and continuous astronomical observation. Simultaneously, advances in onboard artificial intelligence have made real-time processing of photometric data increasingly feasible within spaceborn systems. However, the integration of federated learning into satellite networks introduces significant challenges related to data privacy, communication security, and long-term cryptographic resilience. Existing satellite communication protocols rely heavily on classical public-key cryptography, which is vulnerable to future quantum computing attacks. Given the extended operational lifespan of space missions, this creates a critical security concern for scientific data and collaborative machine learning processes. This paper proposes a quantum-resistant federated learning framework for CubeSat constellations dedicated to real-time exoplanet detection. The proposed architecture integrates lightweight homomorphic encryption based on the learning with errors (LWE) problem with a resource-aware federated learning pipeline optimized for low Earth orbit (LEO) environments. By enabling secure aggregation of encrypted model gradients without exposing raw observational data, the framework preserves both privacy and scientific integrity while maintaining resilience against quantum adversaries. The system architecture further incorporates hierarchical inter-satellite communication, onboard TinyML processing, and FPGA-accelerated cryptographic operations tailored to CubeSat hardware limitations. Experimental evaluations conducted using simulated Kepler and TESS light curve datasets demonstrate that the proposed framework achieves strong detection performance while operating within realistic satellite power, memory, and bandwidth constraints. The results indicate that quantum-resistant secure federated learning is both technically feasible and practically deployable for future distributed space missions. This work establishes a foundation for secure autonomous scientific collaboration in next-generation satellite constellations.***

Keywords: Federated Learning, CubeSats, Post-Quantum Cryptography, Homomorphic Encryption, Exoplanet Detection, Learning with Errors, TinyML, Space Security

I. INTRODUCTION

The discovery and characterization of exoplanets remain among the most important objectives in contemporary astrophysics. Over the past two decades, missions such as Kepler and TESS have transformed planetary science through large-scale observation of stellar systems using transit photometry. Despite their scientific success, conventional monolithic observatories are constrained by high development costs, limited scalability, and restricted observational coverage. As a result, distributed satellite architectures—particularly CubeSat constellations—have emerged as a promising alternative for future exoplanet detection missions.

CubeSats provide several advantages for space-based astronomical observation. Their modular design, low manufacturing cost, and rapid deployment capability allow large constellations to be constructed at a fraction of the cost of traditional missions. Distributed constellations also improve fault tolerance and enable near-continuous sky monitoring across multiple orbital planes. These characteristics make CubeSats particularly attractive for missions requiring persistent photometric observation and large-scale data collection.

At the same time, the increasing availability of onboard AI has enabled satellites to process observational data directly in orbit. Instead of transmitting raw photometric light curves to Earth, CubeSats can locally analyze stellar brightness

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719027

variations using machine learning algorithms. This significantly

reduces communication overhead while enabling near real-time exoplanet detection. Federated learning offers major advantages for distributed space systems, but it introduces several important security and privacy concerns. Model updates exchanged during training may leak sensitive information through gradient inversion attacks, and malicious satellites may intentionally submit poisoned updates to disrupt the learning process. More critically, most existing satellite communication infrastructures rely on classical cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), both of which are vulnerable to future quantum computing attacks.

To address these challenges, this paper proposes a quantum-resistant federated learning framework designed specifically for CubeSat constellations engaged in exoplanet detection.

II. BACKGROUND AND RELATED WORK

2.1 Federated Learning in Space Systems

Federated learning has become an increasingly important paradigm for distributed AI, particularly in environments where centralized data collection is impractical or undesirable. In satellite constellations, federated learning enables multiple spacecraft to collaboratively train machine learning models while retaining observational data locally.

Recent studies have explored the feasibility of federated learning in low Earth orbit (LEO) satellite networks for applications such as Earth observation, intrusion detection, and autonomous navigation.

2.2 CubeSat Constraints and Hardware Limitations

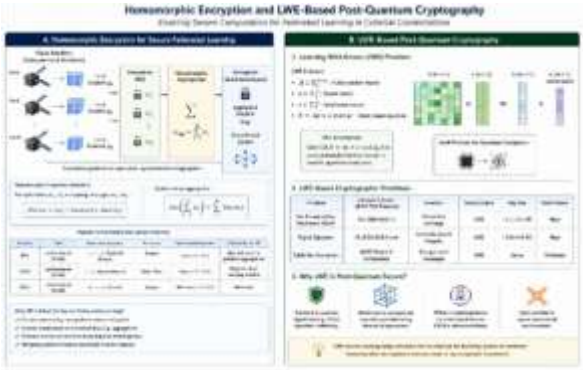
Despite their advantages, CubeSats operate under severe size, weight, Power, and Cost (SWaP-C) limitations. Typical CubeSat platforms possess limited onboard memory, restricted computational capability, and narrow communication bandwidth.

Key operational constraints include the following:

Constraint	Typical CubeSat Range
Memory	1-16 MB RAM
Power Budget	5-12 W
Communication Window	5-10 min/orbit
Radiation Exposure	High
Processing Capability	Limited ARM/FPGA Systems

2.3 Homomorphic Encryption and Post-Quantum Cryptography

Homomorphic encryption enables mathematical operations directly on encrypted data, making it ideal for secure federated learning, especially in learning-based systems. Lattice-based cryptography, especially systems built on the learning with errors (LWE) problem, offers strong resistance against both classical and quantum attacks.



© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719027

III. SYSTEM ARCHITECTURE

3.1 CubeSat Constellation Design

The proposed architecture consists of a distributed constellation of CubeSats operating in sun-synchronous low-earth orbit at an altitude of approximately 600 kilometers. The constellation employs a Walker-Delta configuration to maximize observational coverage and communication redundancy.

Core Components:

- High-precision photometric payload
- TinyML onboard AI processor
- Radiation-hardened FPGA accelerators
- Secure inter-satellite communication modules

- Quantum-resistant cryptographic engine.

3.2 Federated Learning Workflow

The federated learning process operates in iterative rounds:

1. Local light curve processing
2. Gradient computation
3. Gradient quantization
4. LWE-based encryption
5. Secure encrypted transmission
6. Homomorphic aggregation
7. Global model synchronization

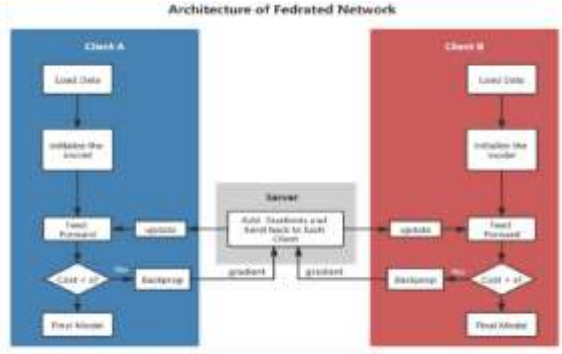
Mathematical Formulation

$$ct_{agg} = \sum_{i=1}^{N} ct_i$$

$$\theta_{t+1} = \theta_t - \eta \cdot \frac{g_{total}}{N}$$

Where:

- ct_i = encrypted gradient
- g_{total} = aggregated gradient
- η = learning rate



IV. PROPOSED QUANTUM-RESISTANT ENCRYPTION FRAMEWORK

4.1 Gradient Quantization

To reduce communication overhead and encryption complexity, gradients are clipped and quantized before encryption.

$$\hat{g}^{(i)} = \frac{g^{(i)}}{\max\{1, ||g^{(i)}||_\infty / C\}}$$

This process minimizes noise accumulation during homomorphic aggregation.

4.2 LWE-Based Encryption

Each gradient vector is encrypted using the following LWE-based formulation:

$$ct^{(i)} = Enc_s(g^{(i)}) = As + \gamma Q_b(g^{(i)})$$

The encryption scheme preserves additive homomorphic properties while remaining resistant to quantum attacks.

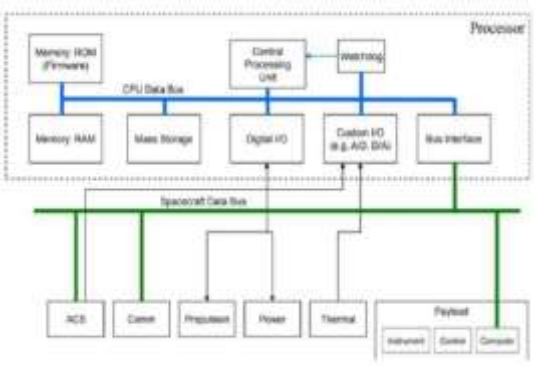
4.3 Resource-Aware Optimization

The framework introduces several optimizations for CubeSat deployment:

Optimization	Purpose
Reduced lattice dimension	Lower computation
INT8 quantization	Reduced memory

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719027

FPGA acceleration	Faster encryption
Lightweight aggregation	Lower bandwidth
Adaptive scheduling	Energy efficiency



V. EXPERIMENTAL SETUP

The framework was evaluated within a realistic orbital simulation environment.

- Orbital mechanics
- Dynamic inter-satellite communication
- Power generation cycles
- Communication latency
- Radiation-aware hardware constraints

The machine learning dataset was derived from Kepler and TESS-style exoplanet light curves.

Dataset Categories

Dataset Type	Description
Confirmed Exoplanets	Verified transit signatures
False positives	Stellar variability and eclipsing binaries
Synthetic signals	Augmented transit injections

VI. RESULTS AND ANALYSIS

6.1 Detection Performance

Metric	Encrypted FL	Unencrypted FL
Detection accuracy	90.26%	96.91%
Encryption time	0.54	0 ms
Decryption time	0.04 ms	0 ms
Communication Expansion	2.876x	1x

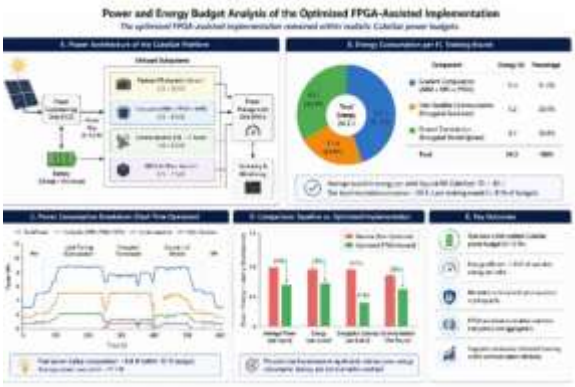
The encrypted federated learning framework maintained strong classification performance while introducing acceptable computational overhead.

6.2 Energy and Latency

Average energy consumption per training round:

Component	Energy Usage
Gradient computation	12.4 J
Inter-satellite communication	6.2 J
Ground transmission	8.7 J
Total	24.3 J

The optimized FPGA-assisted implementation remained within realistic CubeSat power budgets.



VII. SECURITY ANALYSIS

The proposed framework provides resistance against multiple threat vectors:

Threat	Mitigation
Quantum attacks	LWE-based post-quantum encryption

Gradient inversion	Homomorphic encryption
Byzantine poisoning	Secure aggregation validation
Eavesdropping	End-to-end encrypted ISLs
Side-channel attacks	Constant-time cryptographic operations

The probability of overflow during encrypted aggregation remained below the following:

$$P(overflow) < 10^{-6}$$

Demonstrating strong numerical stability and reliable, secure aggregation.

VIII. DISCUSSION

The integration of post-quantum cryptography into CubeSat federated learning introduces a trade-off between security and system efficiency. Stronger encryption increases communication overhead and computational complexity. However, these costs are justified by the long operational lifespans of satellite missions and the increasing threat posed by quantum computing.

Additionally, constellation dynamics such as intermittent connectivity and non-IID data distributions introduce further challenges for federated optimization.

Future work should focus on asynchronous aggregation and adaptive communication scheduling to improve scalability across large orbital networks.

IX. CONCLUSION

This paper presented a quantum-resistant federated learning framework for secure exoplanet detection using CubeSat constellations. By integrating lightweight homomorphic encryption with lattice-based post-quantum cryptography, the proposed architecture enables privacy-preserving collaborative machine learning within realistic satellite resource constraints.

Experimental results demonstrated that the framework achieves strong detection performance while maintaining feasible energy consumption, communication overhead, and computational latency. The system further provides long-term resilience against quantum adversaries, establishing a viable foundation for future autonomous scientific missions in space.

Future work will include:

- Radiation testing of cryptographic hardware
- In-orbit validation experiments
- Hardware-software co-design for FPGA acceleration
- Adaptive asynchronous federated learning
- Standardization of post-quantum satellite protocols

REFERENCES

[1] Bringing Federated Learning to Space. “arXiv Preprint.” Accessed May 19, 2026. https://arxiv.org/html/2511.14889v1.

[2] “Cryptographically Relevant Quantum Computers (CRQCs).” Post-Quantum. Accessed May 19, 2026. https://postquantum.com/post-quantum/crqc/.

[3] “Exoplanet Detection Using Machine Learning.” Monthly Notices of the Royal Astronomical Society. Accessed May 19, 2026. https://academic.oup.com/mnras/advance-article/doi/10.1093/mnras/stab3692/6472249.

[4] “Exoplanet Detection by Machine Learning with Data Augmentation.” arXiv. Accessed May 19, 2026. https://arxiv.org/abs/2211.15577.

[5] “On-board Federated Learning for Satellite Clusters with Inter-Satellite Links.” IEEE Xplore. Accessed May 19, 2026. https://ieeexplore.ieee.org/document/10409275/.

[6] “Over-the-Air Federated Learning in Satellite Systems.” arXiv. Accessed May 19, 2026. https://arxiv.org/abs/2306.02996.

[7] “Post-Quantum Cryptography for Space Systems: Algorithms and Challenges.” Acta Astronautica. Accessed May 19, 2026. https://www.sciencedirect.com/science/article/abs/pii/S0094576526002730.

[8] “Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols.” arXiv. Accessed May 19, 2026. https://arxiv.org/pdf/1910.07557.

[9] Satellite-Based Computing Networks with Federated Learning.” arXiv. Accessed May 19, 2026. https://arxiv.org/pdf/2111.10586.

[10] “TinyML Enhances CubeSat Mission Capabilities.” arXiv. Accessed May 19, 2026. https://arxiv.org/html/2603.20174v1.

[11] “Towards Quantum-Safe Federated Learning via Homomorphic Encryption.” arXiv. Accessed May 19, 2026. https://arxiv.org/html/2402.01154v1.