This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

Submitted to SI on Orbital Edge: Data Centres in Space

Securing the Orbital Edge against Quantum Threats: Use Cases, Challenges, and Research Directions

Gökcan Cantali, *Zürich University of Applied Sciences, CH-8401 Winterthur, Switzerland, and Communication Systems Group, University of Zürich, CH-8050 Zürich, Switzerland*

Dina Abdelhadi, Gürkan Gür, *Zürich University of Applied Sciences, CH-8401 Winterthur, Switzerland*

Saleh Darzi, Attila Altay Yavuz, *Bellini College of Artificial Intelligence, Cybersecurity and Computing, University of South Florida, Tampa, 33620 Florida, USA*

Abstract—The proliferation of low-Earth orbit (LEO) satellites offers opportunities for orbital edge computing and harnessing solar energy for machine learning (ML). In space-based data centers, sensitive and private information will frequently be processed and exchanged in a highly connected, distributed edge-processing environment with wireless links, thereby expanding the attack surface and exacerbating security challenges in current space systems. Concurrently, rapid progress in quantum computing empowers adversaries as well, thereby making quantum threats indispensable to analyze and address with caution, especially in the critical orbital edge applications. This article examines challenges posed by the interplay of the orbital environment, AI/ML, and post-quantum (PQ) security for space data centers. It illustrates this interaction through an evaluation of the overhead associated with a PQ-secure implementation of a concrete orbital AI use case, and provides a review of challenges and future research directions.

Traditionally, satellites have been used primarily for communication and were assumed to provide only limited onboard computation, since their components were designed for long missions and therefore required strong resilience to harsh space environments. However, with the emerging orbital edge paradigm, this perspective is shifting, primarily thanks to declining launch costs and hardware that is more capable and resilient to component risk. As a result, commercial off-the-shelf (COTS) hardware becomes increasingly viable for onboard processing across a range of applications, particularly in low-Earth orbit (LEO) satellites due to lower Earth-to-space latency. Such applications supported by expanding LEO satellite constellations generate vast amounts of valuable data, which enable on-board machine learning (ML)-driven applications and autonomous decision-making towards a future with more agile space systems.

XXXX-XXX © 2026 IEEE
Digital Object Identifier 10.1109/XXX.0000.0000000

In this setting, an emerging avenue for investigation is moving a subset of computationally-heavy operations, such as training or inference artificial intelligence (AI) workloads, to satellites, which benefit from the abundance of solar energy [1]. Furthermore, satellite-assisted AI applications can provide wide-scale coverage for mobile devices via edge connectivity, a property that is difficult to achieve by leveraging terrestrial-only wireless networks. On the other hand, the feasibility of deploying AI workloads on the orbital edge remains an open question, due to many challenges in the space environment such as communication difficulties, high solar radiation, constrained devices, and reduced capability of physical maintenance and control. These challenges necessitate a thorough analysis on the communication and computational constraints, as well as security requirements, for proper operation.

In addition to space-native issues, the rise of quantum computing leads to substantial risks in many digital systems, especially those that operate on large-scale critical systems such as satellite-based orbital edge infrastructures [2]. After all, satellite systems are

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

deployed to remain in orbit for 5-20 years, with limited access for maintenance and updates. Moreover, their ground-satellite communications are broadcast, usually over insecure links. As such, satellite systems are particularly vulnerable to harvest-now/decrypt-later (HNDL) attacks, where malicious entities collect encrypted data now, and store them until technology becomes sufficiently advanced to crack their encryption, making post-quantum (PQ) security an obligation.

Unfortunately, the risk of quantum-powered malicious entities against space systems extends beyond confidentiality. If the public-key infrastructure (PKI) protecting orbital systems is compromised, adversaries could undermine certificate chains, impersonate legitimate entities, and forge authentication for software updates, control traffic, and inter-system communications. This could lead to not only an unauthorized access to space-hosted assets, but also scenarios involving disruption of services via resource depletion or model poisoning. Furthermore, under certain circumstances, the malicious contact may cascade into connected terrestrial components, further endangering Earth-hosted critical infrastructure. However, a naive transition to post-quantum cryptography (PQC) is not straightforward, since the larger keys, signatures, and certificates of current post-quantum (PQ) schemes can introduce communication overhead and fragmentation, making efficient and resilient PQ-secure trust management a central challenge for communicationally challenging space systems. Especially in the scope of emerging orbital edge systems, where space devices process compute-heavy AI workloads, this cost of PQC needs to analyzed in detail for sustainable and secure operation of deployed services.

Given such rationale, this paper tackles these issues and makes the following contributions:

- Highlighting security threats raised by quantum-powered adversaries for space edge systems,
- Proposing a set of AI-focused use cases for the orbital edge, in which PQC can thwart critical security threats,
- Analyzing the overhead of PQC adoption, as well as demonstrating the magnitude and mechanisms of such overhead, by studying a specific deployment example,
- Outlining the challenges of incorporating PQC in space edge systems and laying the foundation of future research directions in this area.

Related Work

This section provides a brief introduction to the topic of PQC and space data centers, while highlighting recent studies on the adoption of PQC in space environments.

PQC and its Adoption into Space Systems

Quantum computing poses a fundamental threat to conventional public-key cryptography [3]. In particular, algorithms such as Shor's algorithm can efficiently solve structured problems, including integer factorization and discrete logarithms, thereby undermining widely deployed schemes such as RSA and elliptic-curve cryptography (ECC). To address this threat, PQC introduces public-key primitives believed to remain secure against both classical and quantum adversaries. Among the candidates are lattice-based schemes such as Dilithium, standardized as ML-DSA, and Falcon for digital signatures, as well as ML-KEM for key encapsulation. Compared with classical schemes, however, PQC primitives typically incur larger public keys, ciphertexts, and signatures, as well as higher computational overhead. These costs are particularly important in space systems, where communication bandwidth, energy, memory, and onboard processing resources are inherently constrained.

PQ-secure authentication and key-establishment mechanisms can be used to derive symmetric session keys, after which bulk data can be protected with symmetric encryption. In this setting, the main PQC overhead occurs during connection establishment, especially during the initial handshake and subsequent rehandshakes triggered by link disruptions, mobility, or handovers. Hence, the frequency of session establishment directly affects the overall cost of deploying PQ-secure protocols. The appropriate PQC protocol depends on the setting. For instance, in an application where multicast or broadcast communication is more prominent, post-quantum group key management and scalable authentication mechanisms [4] might be more beneficial than simple point-to-point PQ-secure key establishment protocols.

Recent works have also investigated the adoption of PQC into space systems. The challenges of PQC fragmentation, handovers, and performance in LEO constellations are discussed in [5]. The study addresses IP-level fragmentation and CPU-level bottlenecks and validates its findings through extensive ns3 simulations. The study also measures the difference in fragmentation levels between Falcon and Dilithium, concluding that implementing a hybrid solution based on Falcon could be ideal for LEO satellites in the orbit.

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

The survey [6] provides a systematic overview on the existing literature of PQC, focusing on its application in space systems. The study reviews existing research from various perspectives and deduces that lattice-based solutions, with ML-KEM and ML-DSA being primary examples, prove to be feasible options for securing resource-constrained satellite systems against quantum threats.

A recent study by Akram *et al.* [7] proposes a lightweight PQ-secure authentication protocol, specifically adhered to the resource-constrained satellite systems. The idea is to utilize physically unclonable functions and hash-based schemes to establish session security, and the protocol's security and efficiency is validated through a formal analysis and experiments.

Orbital Edge and Space-based Data Centers

Deploying data centers in space, as part of the orbital edge paradigm, is a proposal to host IT infrastructure for running services and applications, as well as data storage and AI/ML workloads, onboard satellites to primarily leverage massive amounts of solar energy. Some proposals envision a monolithic design in which all servers and infrastructure are co-located on a single satellite, surrounded by a massive solar array. However, this monolithic approach is fraught with physical difficulties, including the required launch vehicle sizes, challenging in-orbit assembly, and a single point-of-failure possibility.

One key and initial study in this area has been proposed by Arcas *et al.* [1], which uses a satellite-based architecture to host AI datacenters. The illustrated architecture consists of 81 closely spaced LEO satellites in a sun-synchronous orbit. The study shows that it is possible to utilize solar energy almost all the time by placing the orbit in a dusk-dawn zone. In fact, the energy efficiency gains from such a setup drive the primary motivation for AI-based data centers in space. Moreover, a feasibility analysis across multiple dimensions has been conducted to assess the operability of this theoretical architecture, including the radiation resistance of Google's tensor processing units (TPUs), estimated launch costs for LEO satellites, orbital dynamics, and the communication properties of intersatellite links. The study [1] concludes that TPUs can withstand radiation up to five years before suffering significant performance degradation, thus deploying space data centers will be favorable with decreasing launch costs in the near future.

Another recent study by Naser *et al.* [8] has explored the concept of the orbital edge in a more futuristic setting. The proposed architecture consists not only of LEO satellites but also of medium Earth orbit and geostationary Earth orbit satellites, with delay-sensitive space data centers at lower altitudes, whereas delay-tolerant applications are deployed in satellites farther from Earth's surface. Various use cases are considered in the study, namely in-orbit computing, bandwidth minimization, resilient digital backbones, orbital cloud access, and orbital data twins. Overall, the study has laid out a foundation for a visionary space-based data center deployment.

Liu *et al.* have explored the challenges of executing AI workloads in space [9]. The study discusses making COTS hardware more radiation-resistant so they can replace less efficient space-specific units. The authors also highlighted major components for a more reliable and robust computing architecture in space, along with an implementation of a visual AI inference as a small use case.

One of the use cases for space data centers is the execution of ML on satellites, which includes privacy-preserving distributed learning paradigm, such as federated learning (FL). In that regard, the security of FL across LEO constellations is addressed in [10].

Given this variety of orbital edge applications, understanding the tradeoffs of PQ-secure orbital edge is critical. Nevertheless, few studies focus on the post-quantum cybersecurity aspects of the orbital edge, despite a growing body of research on AI workloads in space, which drives the main motivation of this paper.

Quantum Computing Threats for the Orbital Edge

This section investigates the threats against orbital edge systems posed by potential future adversaries with access to quantum computers sufficiently powerful to break traditional PKI systems. Figure 1 consolidates these threats in an illustration, where attackers target a space-based data center, comprising various components such as ML, inference, storage, and relay units in the absence of PQ-secure PKIs. Note that this paper focuses on quantum-computing threats, rendering traditional issues, such as debris collision or DoS attacks, out of scope.

Eavesdropping on Data Transmitted over ISLs and GSLs

HNDL attacks mean that the data transmitted over the GSLs and ISLs by a satellite launched today with RSA or ECC-based security may be decrypted once a cryptographically relevant quantum computer

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

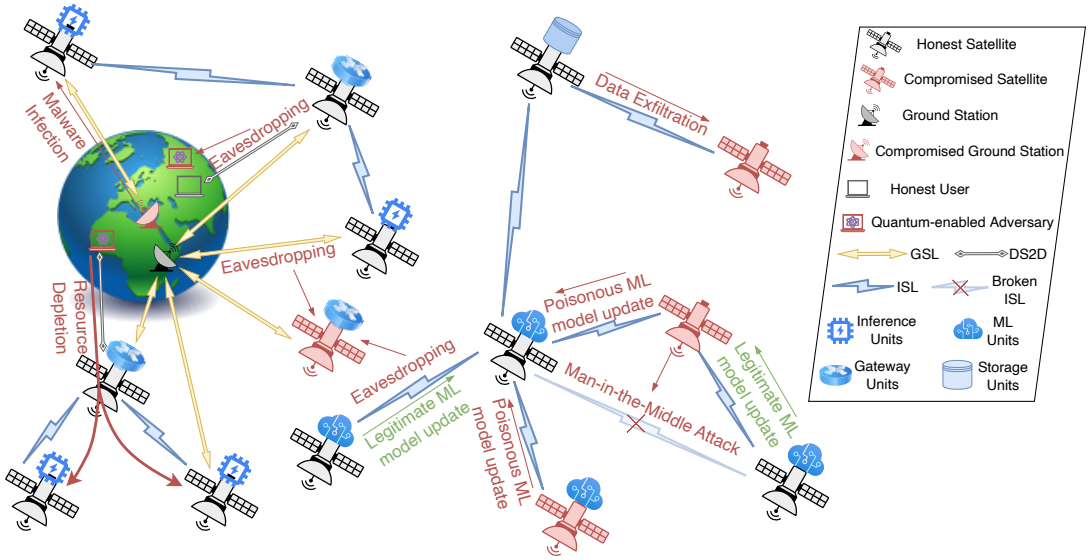

FIGURE 1: The threat landscape stemming from quantum computing against the orbital edge paradigm.

exists, possibly within the satellite's mission lifetime. Attackers may also intercept non-PQ-safe TLS traffic and use a quantum computer to obtain the symmetric key resulting from the exchange, jeopardizing even symmetric key-encrypted data. The orbital edge setting specifically exacerbates the issue of HNDL threats, as the expected deployment lifetime of these applications is several years, requiring high crypto-agility for protection against future threats. Moreover, the volume and critical nature of data exchanged over ISLs and GSLs in the orbital edge setting, such as confidential ML model parameters, makes PQC necessary to ensure the security of ISLs and GSLs in orbital edge.

Data Exfiltration from Data Center Storage

Similarly, a quantum-powered adversary may use broken PKI to spoof an authorized user then harvest the data from the database, use the spoofed user's read access to get past data at rest encryption to receive decrypted data, and even harvest stored relevant symmetric keys.

Compromising Units via Malware Infection

Quantum computing-powered adversaries can exploit RSA- or ECC-based PKI to obtain unauthorized access and send malicious telecommands to a satellite. A malware infection or an advanced persistent threat could be spread to a satellite, completely compromising its integrity and leading to catastrophic outcomes. While this threat exists for all space systems without PQC-support, orbital edge deployments consist of large distributed systems with highly interactive components, increasing the attack surface significantly. Relying on a big constellation of satellites means that each node is a potential target of cyber-physical attacks, de-orbiting attacks, or a complete takeover.

Disrupting Distributed ML Operations via Model Poisoning

Unlike traditional space systems, space-hosted data centers are expected to train AI models. Note that AI in this case refers to an ML model, which may include generative AI. Due to the sensitivity of training data and resource constraints, consolidating data in a single space unit may be infeasible, thus requiring distributed learning methods, such as FL, to be leveraged instead. Under such privacy-preserving cases, an adversary that manages to compromise an ML unit, via quantum computing, may deliberately upload incorrect model parameters, maybe through a backdoor attack [11], to poison the model as shown in Figure 1. Another possibility is to use a compromised relay unit to perform a man-in-the-middle attack, hijacking ISLs and GSLs, and replace the honest model upload with a malicious one. Such actions degrade the trained model and disrupt the service unless PQC is used to secure the PKI and communication against quantum attacks.

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

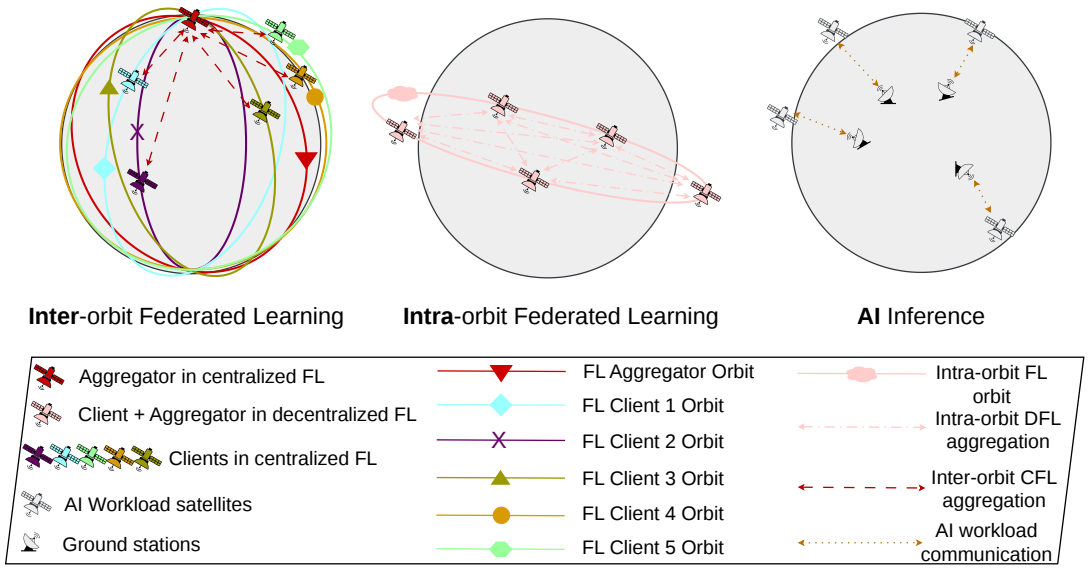

FIGURE 2: An overview of different AI-focused use cases involving space data centers.

Resource Depletion due to Onboard Processing of AI Workloads

A malicious entity can forge the identity of an honest one, and deliberately request consecutive compute-intensive tasks, leading to the depletion of the resources in the satellite unit and significantly impacting the operation of the data center. For this reason, authorization and access protocols must employ PQ-resilient schemes to prevent unauthorized adversaries from accessing services and carrying out critical denial of sustainability attacks.

AI-focused Use Cases for Space Data Center Deployments

Orbital edge computing can serve as an essential component to connect edge IoT devices, satellite nodes, users, and ground stations, while supplying critical infrastructure for AI workloads originating from data collected by these network nodes. Due to its diverse region of impact, the application area of orbital edge varies significantly.

Summary of Use Cases

The AI workloads to be served in space data centers rely on ML pipelines with primarily two phases, namely, training and inference, both of which can be separate use cases for orbital edge applications.

AI model inference: Although training is usually the most resource-intensive part of AI model development, the long-term use of these models means the inference phase can also consume as much energy and incur as much computational overhead as the training phase. Consequently, offloading inference operations to space systems can also be beneficial in the long run. However, for inference-only workloads, communication over GSLs is critical to analyze due to mainly two factors: large input requests or output responses, and longer response time of AI workloads leading to inevitable handover operations.

Training models: Training AI models in space-based data centers is likely to be carried out in a distributed fashion, where FL can serve as a key enabler for distributing the computational load in a privacy-preserving manner. Design choices and challenges in such a system depend on various parameters, such as the topology, the trust model, and the number of unique entities in the system. When multiple parties are involved, additional privacy mechanisms might be required, such as secure multi-party computation, differential privacy, or homomorphic encryption. Regarding the topology, a space-located FL pipeline can be categorized into two settings: where satellites occupy the same orbital plane or different orbital planes, referred to as intra-orbit FL and inter-orbit FL, respectively.

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

The consolidation of the aforementioned orbital edge use cases is illustrated in Figure 2. One common design factor in all of them is that the communication needs to be quantum-safe, such that quantum-powered malicious entities would not be able to tamper with or eavesdrop on sensitive application data. However, PQ-secure adaptations of these protocols will incur additional overhead that needs to be analyzed.

Case Study on PQ-secure Inter-orbit FL

Communication between the satellites is primarily secured by means of PQ-secure mutual TLS (mTLS). Although pre-symmetric keys can also be used, TLS enables the replacement of older satellites, the dynamic adjustment of constellation size, the revocation of rogue satellites' access, and the rotation of keys to prevent key leakage, with the additional cost of session re-establishment. Such cost varies significantly based on the conditions, as a PQ-TLS handshake may need to be established only once per TLS session lifetime for constellations with a stable link, whereas the connection may need to be constantly torn and re-established in dynamic topologies.

To understand the communication overhead needed by PQ-secure TLS connection, we consider a scenario where the orbiting satellites gather imagery or sensory data as they orbit the earth, then apply FL to the unlabeled, streamed data in rounds when their positions are all in range with the aggregator satellite (within 5000 km to ensure a line-of-sight), and we assume the inter-orbit FL case with five clients shown in the leftmost panel of Figure 2. We utilize the setting of self-supervised, FL of unlabeled, streamed data discussed in [12], where the weights of a ResNet-18 network plus a small predictor network, form the communicated messages between the server and the clients every round. The ResNet-18 model weights constitute a communication overhead of about 45 MB in each direction. Another study [13] proposes a communication-efficient FL approach that reduces the communication cost of ResNet-18 by a factor of 356 by communicating only residuals. By applying the approach of [13] into the unsupervised setting of [12], it is assumed that the communication cost is reduced to approximately 0.13 MB per round, per direction.

If all five client satellites are back in range of the aggregator before the TLS session lifetime ends, then there is no need for restablishing the handshake, and the communication overhead for resumption is assumed negligible, depending on the TLS session resumption mode used. However, when the TLS session expires, at the next round, the client and aggregator satellite need to restablish an mTLS session, with a TLS communication overhead depending on the chosen signature algorithm and key exchange mechanism. The session lifetime is determined by a combination of the orbital geometry and a tradeoff between the required security level, as a shorter lifetime means higher security guarantees, albeit at the cost of more communication overhead due to repeated handshakes.

For our use case study, which is illustrated in the leftmost panel of Figure 2, we consider a constellation at an altitude of 550 km, and we leverage the `SGP4` [14] package to compute how often the whole constellation is in range of the aggregator in order to allow FL rounds to take place. For this particular constellation, all clients are in range of the aggregator satellite approximately once every 47-48 minutes on average, and each contact lasts about 11.5 minutes. Furthermore, we focus on the example discussed earlier in [12], in which 300 training rounds are conducted. We take this as an indicative value, even though it may change as the application, dataset, and other scheme details vary. We assume that the data for each round is collected during the orbit, and is then used for one round of training at each contact window. We consider two session lifetime settings: either a new TLS handshake is required at every contact, or a lifetime of 24 hours.

Table 1 demonstrates the overhead due to the extra TLS handshakes. The extent to which the demonstrated communication overhead stresses the system depends on various factors, such as the number of clients, available power for communication, as well as the quality of the communication channel. For example, if the aggregator is on earth, the GSL channel quality will be much worse than an ISL, making communication overhead more problematic. Thus, depending on the setting the PQC overhead may or may not be acceptable for a certain system.

Challenges and Research Directions in PQ-Secure Orbital Edge

Integrating PQ security into space-hosted data centers is not merely an algorithm replacement problem; it is a constrained-systems challenge involving communication overhead, computation cost, latency, hardware limitations, and key-management complexity.

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

TABLE 1: Additional overhead of repeating mTLS handshake under different settings, for two cases: session lifetime of 24h and a new handshake for every connection. For 300 FL rounds, the former requires 10 handshakes, while the latter requires 300 handshakes. The communication overhead of one TLS handshake is determined using `OpenSSL 3.6.2` software package, assuming a certificate chain with two intermediate certificate authorities.

Setting	TLS handshake total bytes on wire	TLS session lifetime	avg. TLS overhead per round per client (bytes)	Ratio of TLS overhead per client to FL communication overhead	
				sending model weights uncompressed ([12])	sending model residuals ([12]+[13])
ECDSA-p256, ECDHE-X25519	4,828	new handshake every connection	4,828	0.005%	1.86%
		24 hours	161	0.00018%	0.06%
Falcon512, ML-KEM-512	18,941	new handshake every connection	18,941	0.02%	7.285%
		24 hours	632	0.0007%	0.243%
ML-DSA-44, ML-KEM-512	39,767	new handshake every connection	39,767	0.044%	15.295%
		24 hours	1,326	0.0015%	0.51%

Networking Challenges of PQC in the Orbital Edge

In the orbital edge, larger cryptographic artifacts can increase bandwidth consumption, trigger packet fragmentation beyond the maximum transmission unit, and add further round-trip delay [5]. These delays could accumulate in long-running ML operations, such as an FL process with multiple rounds, and depending on the setting, may cause substantial communication overhead over time, as shown in Table 1. Moreover, the rapid movement of LEO satellites causes frequent handovers in communication between Earth and space, which is exacerbated in the orbital edge due to the higher processing time required for certain service requests. These issues can be alleviated via smaller PQC certificates [15], as well as smart and scalable handover techniques [16], respectively.

PQ-secure communication sessions

Successfully establishing PQ-secure TLS or other authenticated session-establishment protocols over ISLs may be difficult not only because of larger handshakes, but also because these links rely on frequent pointing, acquisition, and tracking. Furthermore, in addition to PQ-secure TLS for point-to-point channels, PQ-secure authentication and key establishment are also required in a space data center with highly interdependent components. Thus, the challenge also includes scalable key distribution, certificate validation, and trust management across satellites and terrestrial infrastructure. Hardware-rooted trust may help in such settings [17], though it introduces additional challenges regarding radiation robustness, secure provisioning before launch, access revocation and update procedures, and deployment at constellation scale.

Space-Qualified Hardware for Onboard PQC

On space-qualified hardware, the computational cost of PQ routines can be non-trivial given the limited capability of radiation-hardened processors. This trade-off between fault-tolerance and computational capability can be addressed by hybrid and hardware-aware security stacks as well as the implementation of fault-tolerant PQC protocols [18] to identify and correct radiation-induced errors. Another potential issue, especially present in space data centers with AI workloads, is the possibility of energy depletion. This issue is further aggravated with PQC computation [19] and transmission overhead. The utilization of sun-synchronous orbits, specifically dusk-dawn ones, is the primary means to alleviate the negative impact here.

Crypto-Agility Needs in Space

Satellite maintenance needs to be conducted in orbit, necessitating crypto-agility and an easy switch between algorithms or components of security modules, in case vulnerabilities are found within existing ones. Nevertheless, it is a challenging task to address various aspects of crypto-agility [20], including flexible design, hardware reprogrammability, and software component update. This challenge becomes even more evident in space-hosted data centers, where a certain level of isolation across services and virtual resource utilization on servers is expected due to the need to serve multiple users. Therefore, providing crypto-agility in the orbital edge should also consider flexible updates and access control mechanisms.For this reason, general crypto-agility frameworks [6] are needed to establish and validate requirements, both for traditional space systems and orbital edge deployments.

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

TABLE 2: Challenges of applying PQC for space data centers in the orbital edge

Area	Challenge	Source	Description	Mitigation
Networking	Higher fragmentation	AI workload	PQC significantly increases certificate chain sizes [5], hence the number of fragmented packets, causing communication overhead especially in long-term ML operations.	Implementing PQC algorithms with more efficient and compact signatures [5]
Networking	Frequent handovers	Orbital environment & AI workload	Frequent handovers, caused by fast-paced LEO satellites and time-consuming AI workloads, exacerbate the communication overhead of PQC.	Utilizing smart and scalable handover management [16] mechanisms alongside PQC deployments
Hardware	Solar radiation	Orbital environment	While space data centers require special hardware against solar radiation, expensive PQC computations perform better with COTS hardware.	Adopting hybrid hardware stacks as well as the development of fault-tolerant PQC algorithms [18] against radiation-induced errors
Hardware	Energy depletion	AI workload	When expensive PQC protocol executions are combined with intense AI workloads, the chance of critical energy depletion rises [19].	Harvesting continous energy via sun-synchronous dawn-dusk orbits [1] and deploying more efficient radiation-resistant hardware
Security	PQ-secure communication	Orbital environment	Establishing PQ-secure sessions and deploying PQ-secure authentication and key establishment is challenging due the characteristics of an orbital environment.	Using hardware-rooted trust, freshness validation, unlinkable request design, and symmetric session protection for subsequent traffic [17]
Security	Crypto-agility	Orbital environment	Switching security algorithms or security modules must be performed on in-orbit satellites, due to infeasability to landing them back on Earth	Implementing crypto-agility frameworks for the ability to perform flexible updates or adjustments on the security mechanisms [6]

In the context of PQC, orbital data centers, and AI workloads, Table 2 consolidates and summarizes relevant challenges and potential solutions for each.

Conclusion

In this article, we have explored the emerging concept of space data centers through a post-quantum security perspective. Possible AI use cases regarding the orbital edge paradigm have been discussed, as well as relevant quantum-computing security threats, with a highlight on why applying PQC is essential for securing space systems and satellite communications. Through a quantitative analysis on an FL-based use case, the study has found that the cost of PQC communication overhead, under certain settings and configurations, could reach up to 15% of FL model communication data overhead. However, in many other cases, the analysis has yielded an overhead less than 2%, indicating that the severity of the added overhead varies widely depending on the setting. Finally, the challenges of securing space data centers in the post-quantum era have been outlined, and promising research directions have been identified to alleviate the negative impact of integrating PQC for AI-focused space data centers.

ACKNOWLEDGMENTS

This work has received co-funding from the NSF and SNSF, in the framework of the SATUQ project under SNSF (Grant No 10000409) and NSF (ECCS 2444615).

REFERENCES

1. B. A. y Arcas *et al.*, "Towards a future space-based, highly scalable AI infrastructure system design," 2025.
2. A. Tiwari and A. K. Gupta, "Mitigating quantum threats in space domain: Challenges and the role of post-quantum cryptography," in *Proc. 2025 IEEE Space, Aerosp. Defence Conf. (SPACE)*, 2025, pp. 1–6.
3. M. J. Hossain Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A review of quantum cybersecurity: Threats, risks and opportunities," in *Proc. 2022 1st Int. Conf. AI Cybersecur. (ICAIC)*, 2022, pp. 1–8.
4. F. Samiullah, M.-L. Gan, S. Akleylek, and Y. Aun, "Post-quantum group key management in IoTs," in *Proc. 2023 25th Int. Multitopic Conf. (INMIC)*, 2023, pp. 1–6.
5. Y. E. Kwon and J. W. Yoon, "The 1-RTT penalty: Quantifying the recurring cost of PQC fragmentation

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MIC.2026.3754633

in LEO handovers and ISLs," in *Proc. Workshop Secur. Space Satell. Syst. (SpaceSec)*, San Diego, CA, USA, Feb. 2026.

6. H. Kim, "Post-quantum cryptography for space systems: Algorithms, implementation, and design constraints—a systematic survey," *Acta Astronaut.*, 2026.
7. M. A. Akram, A. K. Biswas, M. O'Neill, A. Khalid, and A. N. Mian, "HBQS: Lightweight post-quantum secure authentication for satellite networks leveraging hardware TRNG and PUFs," *IEEE Internet Things J.*, vol. 13, no. 11, pp. 25 256–25 273, 2026.
8. S. Naser *et al.*, "From connectivity to multi-orbit intelligence: Space-based data center architectures for 6G and beyond," *arXiv preprint arXiv:2603.18601*, Mar. 2026.
9. Y. Liu, Y. Han, H. Li, S. Gu, J. Qiu, and T. Li, "Computing over space: Status, challenges, and opportunities," *Engineering*, vol. 54, pp. 20–25, 2025.
10. M. Elmahallawy, T. Luo, and M. I. Ibrahem, "Secure and efficient federated learning in LEO constellations using decentralized key generation and on-orbit model aggregation," in *Proc. GLOBECOM 2023 – IEEE Global Commun. Conf.*, 2023, pp. 5727–5732.
11. G. Rahmanian, P. Madani, and C. M. AM, "Applying patch-based backdoor attacks to in-orbit federated learning for satellite constellations," in *Proc. 2026 IEEE Aerosp. Conf. (AERO)*, 2026, pp. 1–10.
12. J. Shi, Y. Wu, D. Zeng, J. Tao, J. Hu, and Y. Shi, "Self-supervised on-device federated learning from unlabeled streams," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 42, no. 12, pp. 4871–4882, 2023.
13. R. Song, L. Zhou, L. Lyu, A. Festag, and A. Knoll, "ResFed: Communication efficient federated learning by transmitting deep compressed residuals," *arXiv preprint arXiv:2212.05602*, 2022.
14. D. Vallado and P. Crawford, "SGP4 orbit determination," in *Proc. AIAA/AAS Astrodyn. Specialist Conf. Exhib.*, 2008, p. 6770.
15. P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum tls without handshake signatures," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1461–1480.
16. X. Luo, H.-H. Chen, and Q. Guo, "LEO/VLEO satellite communications in 6G and beyond networks-technologies, applications, and challenges," *IEEE Netw.*, vol. 38, no. 5, pp. 273–285, 2024.
17. M. Bakyt, L. La Spada, K. Moldamurat, Z. Kadirbek, and F. Yermekov, "Review of data security methods using low-earth orbiters for high-speed encryption," in *Proc. 2024 4th Int. Conf. Ubiquitous Comput. Intell. Inf. Syst. (ICUIS)*, 2024, pp. 1366–1375.
18. E. Johnson, K. Crabb, J. Leiden, and D. Hamilton, "RRPQ-SCP: Radiation-resilient post-quantum satellite communication protocol," in *AIAA AVIATION 2026 Forum*, 2026, p. 4226.
19. C. A. Roma, C.-E. A. Tai, and M. A. Hasan, "Energy efficiency analysis of post-quantum cryptographic algorithms," *IEEE Access*, vol. 9, pp. 71 295–71 317, 2021.
20. J. Mähn, M. Müller, and K. Zielinski, "Crypto agility definitions for space systems," in *Proc. 2025 Secur. Space Syst. (3S)*, 2025, pp. 1–5.

Gökcan Cantali is a research assistant at Zürich University of Applied Sciences (ZHAW), and a Ph.D. student at the University of Zürich (UZH), Switzerland. His research interests include network security, sustainable computing, and privacy-preserving distributed learning.

Dina Abdelhadi is a researcher at Zürich University of Applied Sciences (ZHAW), Switzerland. Her research interests include quantum information theory, quantum error correction, and satellite networks.

Gürkan Gür is a senior lecturer at Zürich University of Applied Sciences (ZHAW), Switzerland. His research interests include Future Internet, information security, critical infrastructure protection, and next-generation wireless networks.

Saleh Darzi (Graduate Student Member, IEEE) is a Ph.D. Candidate in the Bellini College of Artificial Intelligence, Cybersecurity, and Computing at the University of South Florida. His research pursuits include post-quantum and applied cryptography, network security, and privacy of IoT and Blockchain.

Attila A. Yavuz (Senior Member, IEEE) received the Ph.D. degree in computer science from North Carolina State University in 2011. He is currently an Associate Professor with the Bellini College of Artificial Intelligence, Cybersecurity, and Computing, University of South Florida (USF), where he also directs the Applied Cryptography Research Laboratory.

Authorized licensed use limited to: University of South Florida. Downloaded on November 23,2026 at 18:31:43 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.