International Journal of Innovative Scientific & Engineering Technologies Research 13(4):234-247, Oct,-Dec., 2025

 www.seahipublications.org **ISSN: 2360-896X**

doi:10.5281/zenodo.17930491

Cloud Computing for Space Security: A Critical Review of Threat Mitigation and Access Control

Sopuruchukwu Camillus Ejiofor Onu, T. K Anyachebelu, Steven I. Bassey, Gilbert I.O. Aimufua

Center for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

ABSTRACT

The increasing reliance on cloud computing in space operations has introduced unprecedented efficiencies and capabilities. However, it has also exposed mission-critical systems to a new frontier of cybersecurity threats. This article provides a critical review of the security challenges at the intersection of cloud technology and space networks, with a specialized focus on threat mitigation and access control. By analyzing existing literature, industry reports, and documented cyber incidents, this paper examines the unique vulnerabilities of space-cloud architectures, such as those related to data integrity, confidentiality, and availability. It evaluates the effectiveness of current security paradigms, including Zero Trust Architecture (ZTA), and proposes a comprehensive framework for bolstering the resilience of space assets. The findings indicate that while significant progress has been made in adapting terrestrial security models for space applications, substantial gaps remain in addressing the distinctive constraints of the space environment, such as high latency and intermittent connectivity. This paper concludes by outlining the key contributions to the field, which include a synthesized analysis of the threat landscape and a set of actionable recommendations for developing robust, space-tailored security protocols.

Keywords:Cloud Computing, Space Security, Cybersecurity, Threat Mitigation, Access Control, Zero Trust Architecture, Satellite Systems

1. INTRODUCTION

The rapid integration of cloud computing into space operations marks a transformative shift in how space missions are designed, managed, and executed. The ability to process, store, and disseminate vast volumes of data in real-time has unlocked new possibilities for satellite communication, Earth observation, and deep-space exploration [1]. However, this growing dependence on cloud infrastructure has also introduced a complex and critical set of security vulnerabilities. Space assets, which were once considered isolated and physically secure, are now part of a globally interconnected network, making them prime targets for a wide range of cyber threats [2].

The statement of the problem is clear: the very technologies that enable the next generation of space exploration also expose it to significant risks. High-profile cyber incidents, such as the 2022 attack on the ViaSat KA-SAT network, have demonstrated the tangible consequences of these vulnerabilities, disrupting services across Europe and highlighting the potential for space-related cyber-attacks to have far-reaching geopolitical implications [3]. Furthermore, reports from government agencies like the U.S. Government Accountability Office (GAO) and the NASA Office of the Inspector General have consistently pointed to deficiencies in the cybersecurity posture of space systems, including inadequate threat mitigation strategies and weak access control mechanisms [4, 5].

This article addresses the urgent need for a specialized security framework tailored to the unique characteristics of the space-cloud environment. It seeks to answer the following research questions:

1. How can cloud-based threat mitigation strategies be effectively adapted and implemented to secure space operation networks against sophisticated cyberattacks?
2. What access control mechanisms are most suitable for protecting the integrity of data and systems in a distributed, high-latency, and resource-constrained space environment?
3. What are the primary security risks inherent in the adoption of cloud computing for space operations, and how can they be addressed through innovative architectural designs?

To answer these questions, this paper provides a comprehensive review and analysis of the current state of cloud security in space operations. The scope of this study is focused on civil and commercial space activities, and it synthesizes information from academic literature, industry best practices, and publicly available incident reports. By focusing on the two fundamental pillars of threat mitigation and access control, this research aims to provide a robust conceptual framework for securing the next generation of space-based assets. The significance of this study lies in its potential to inform the development of new security policies, guide the implementation of more resilient space-cloud architectures, and contribute to the overall safety and sustainability of the space domain.

2. Literature Review

The convergence of cloud computing and space operations is a relatively new and rapidly evolving field. While the benefits of this integration are widely acknowledged, the security implications are still being fully understood. This section provides a review of the existing literature, focusing on the conceptual framework of cloud security in space, the key pillars of threat mitigation and access control, and the emerging paradigm of Zero Trust Architecture (ZTA).

2.1. Conceptualizing Security in Space-Cloud Systems

The academic discourse on cloud security has traditionally focused on terrestrial applications. However, the unique characteristics of the space environment—such as high latency, limited bandwidth, and the critical nature of the assets involved—necessitate a specialized approach [6]. The conceptual framework for space-cloud security, as outlined in the literature, is built upon the foundational principles of confidentiality, integrity, and availability (the CIA triad), but with a heightened emphasis on resilience and mission continuity [7].

Several studies have highlighted the need for a holistic security model that extends beyond the traditional perimeter-based defense. For instance, Ali et al. (2015) provided a comprehensive survey of the security issues inherent in cloud computing, emphasizing the risks associated with multi-tenancy and the loss of administrative control [8]. While their work was not specific to the space domain, it laid the groundwork for understanding the fundamental vulnerabilities of cloud architectures. More recent studies have begun to address the specific challenges of space-cloud integration. For example, Amara et al. (2017) explored the architectural principles and key security requirements for cloud computing in critical infrastructure, offering a more tailored perspective that is applicable to space systems [9].

2.2. Threat Mitigation in the Space Domain

Threat mitigation in space-cloud systems is a multi-faceted challenge that involves the proactive identification, analysis, and neutralization of a wide range of cyber threats. These threats can range from denial-of-service (DoS) attacks and signal spoofing to malware and insider threats [10]. Recent incidents underscore the urgency of this challenge. In 2022, the AcidRain malware attack on ViaSat's KA-SAT satellite network disabled thousands of modems across Europe, demonstrating the real-world impact of inadequate threat mitigation [20]. Similarly, researchers have documented spillover attacks where satellite disruptions cascaded into civilian infrastructure, including German wind turbines losing operational control [21]. More recently, emerging malware strains such as AcidPour have targeted embedded devices and IoT systems in space-edge environments, while ransomware infection vectors in orbit have shown a 33 percent success rate in emulated Low Earth Orbit (LEO) systems [22].

The literature emphasizes the need for a layered defense strategy that incorporates several key components. **Threat Identification and Intelligence** relies on real-time threat intelligence sourced from global cyber incident databases, anomaly detection engines, and predictive analytics to identify malicious activity [11]. The use of AI-driven tools is becoming increasingly prevalent, as they can adapt to the evolving threat landscape and detect novel attack vectors. **Risk Assessment and Prioritization** is crucial given the limited resources available in space systems. Threats must be prioritized based on their potential impact and likelihood of occurrence, involving a continuous process of risk assessment that informs the allocation of security resources [12]. **Preventive Security Mechanisms** include the implementation of controls such as firewalls, encryption, and network segmentation. In space communications, end-to-end encryption is particularly vital for protecting data in transit, and misconfigured VPN appliances—which have been exploited to enable lateral movement to control systems—must be carefully managed [13, 22]. **Anomaly Detection and Monitoring** involves continuous scanning of network traffic and system behavior to detect anomalies that may indicate a security breach. Machine learning algorithms are increasingly used to establish a baseline of normal activity and identify deviations that could signal an attack [14].

2.3. Access Control as a Foundational Pillar

Access control is another critical pillar of space-cloud security. In an environment where a single unauthorized action can have catastrophic consequences, it is essential to ensure that only authorized entities can access sensitive data and systems. The literature highlights several key features of effective access control mechanisms. **Identification and Authentication** form the foundational layer, with the process of verifying the identity of users and devices serving as the first line of defense. Multi-factor authentication (MFA) is widely regarded as a best practice, as it provides an additional layer of security beyond traditional passwords [15]. **Authorization Mechanisms** determine what level of access an entity is permitted once their identity has been authenticated. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are two common models for enforcing authorization policies [16]. The **Principle of Least Privilege** dictates that users and systems should only be granted the minimum level of access necessary to perform their functions. By limiting access rights, this principle can significantly reduce the attack surface and mitigate the risk of insider threats [17].

2.4. The Emergence of Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) represents a paradigm shift in cybersecurity. It is based on the principle of "never trust, always verify," which means that no entity is granted implicit trust, regardless of its location or credentials. In the context of space-cloud systems, where the network perimeter is becoming increasingly blurred, ZTA is a particularly relevant and promising approach [18]. The CISA report on Space Systems Security and Resilience Landscape (2024) has identified ZTA as a critical framework for addressing the unique security challenges of space environments, providing guidance for both existing systems and new acquisitions [23].

The implementation of ZTA in space-cloud environments involves several key strategies, including continuous verification of user identities, dynamic access controls, and micro-segmentation of networks. By eliminating implicit trust, ZTA can significantly reduce the risk of unauthorized access and lateral movement within the system [19]. Emerging frameworks such as the FORTRESS (Framework for Operational Resilience and Trust in Space Systems) have demonstrated practical implementations of ZTA principles in satellite operations. FORTRESS leverages kernel-level runtime security through KubeArmor and integrates workload identity management using SPIFFE (Secure Production Identity Framework for Everyone) to enforce fine-grained policies at the system-call level [24]. This approach ensures that all workloads are authenticated, only minimum necessary permissions are granted, and policies are continuously validated during build, deployment, and runtime phases. While the adoption of ZTA in the space domain is still in its early stages, it is widely regarded as a critical component of any future-proof security architecture, particularly for containerized satellite systems and distributed space-cloud environments.

2.5. Ground Segment Security and Cloud Integration

The ground segment of space systems—encompassing ground stations, mission control centers, and data processing facilities—represents a critical interface between space assets and cloud-based infrastructure. Recent research has highlighted the unique security challenges associated with Ground Station as a Service (GSaaS) models, where multiple operators share cloud-based ground station infrastructure [25]. The adoption of GSaaS is rapidly expanding due to its cost efficiencies, scalability, and operational flexibility. Cloud integration improves accessibility, enables seamless handovers across global ground stations, and optimizes resource utilization. However, this transition introduces new cyber security challenges that require careful management. The shared responsibility model in cloud services requires clear delineation of security obligations between GSaaS providers and users to prevent accountability gaps. Legacy systems pose an additional challenge, as many satellite systems were not designed with modern cybersecurity practices in mind. Integrating these systems with cloud-based solutions requires careful consideration to avoid exposing outdated interfaces and insecure protocols [25].

3. Conceptual Framework and Models

This study is grounded in a conceptual framework that integrates principles from cybersecurity, cloud computing, and space systems engineering. The framework, depicted in Figure 1, illustrates the interplay between the key components of a secure space-cloud ecosystem. It highlights the central role of threat mitigation and access control as the foundational pillars of security, while also incorporating the emerging paradigm of Zero Trust Architecture (ZTA) as a critical enabler of a proactive and resilient security posture.

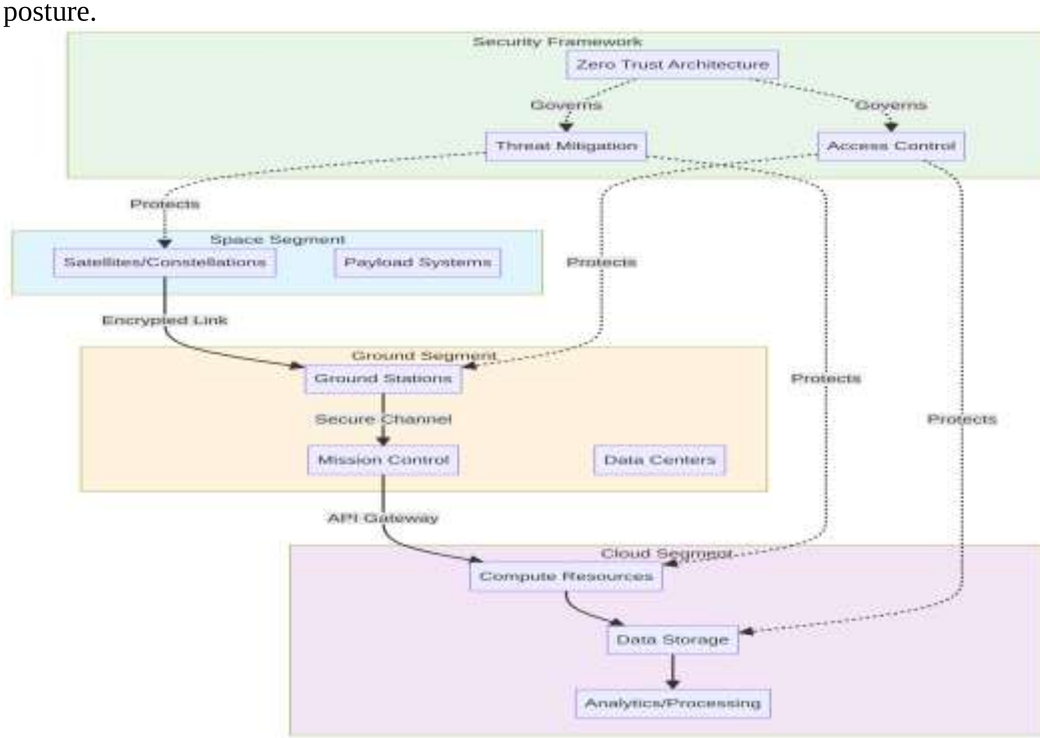

Figure 1: Conceptual Framework for Secure Space-Cloud Operations

3.1. The MITRE ATT&CK Framework for Space

While not explicitly designed for space systems, the MITRE ATT&CK framework provides a valuable model for understanding and categorizing adversary tactics and techniques. The adaptation of this framework for the space domain allows for a more systematic approach to threat modeling and the development of targeted mitigation strategies. The ATT&CK for Space framework would encompass tactics such as initial access (e.g., exploiting ground station vulnerabilities), execution (e.g., injecting malicious code into satellite command sequences), and impact (e.g., disrupting satellite operations or denying service).

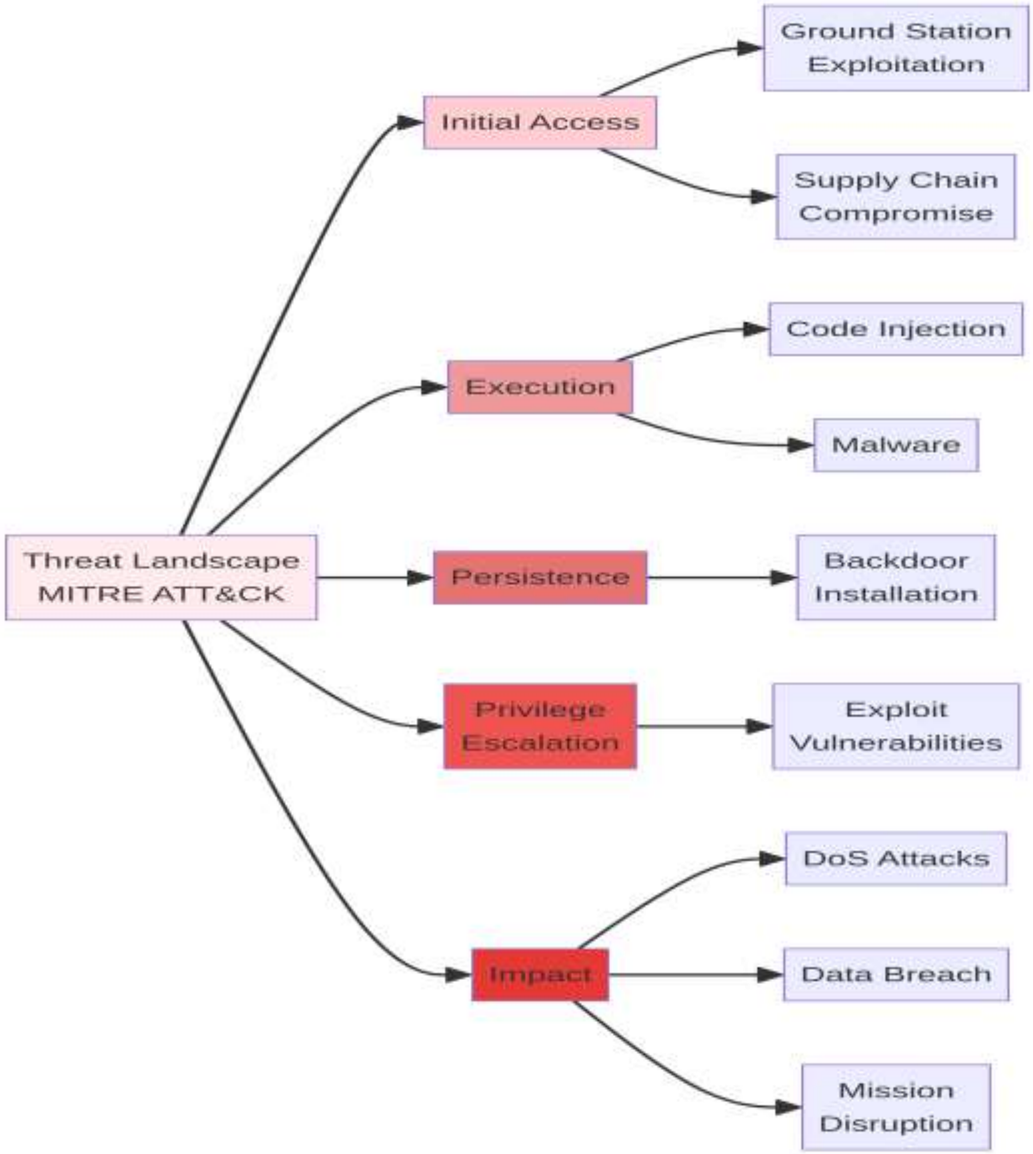

Figure 2: Adapted MITRE ATT&CK Framework for Space

3.2. The Purdue Model for ICS and its Adaptation to Space

The Purdue Model for Industrial Control Systems (ICS) offers a useful reference architecture for segmenting and securing critical infrastructure. While space systems are not identical to terrestrial ICS, the principles of network segmentation and the separation of operational technology (OT) from information technology (IT) are highly relevant. An adapted Purdue Model for space would create distinct security zones for the space segment (satellites), the ground segment (ground stations and control centers), and the cloud segment (data processing and storage), with strict access controls and monitoring at the boundaries between these zones.

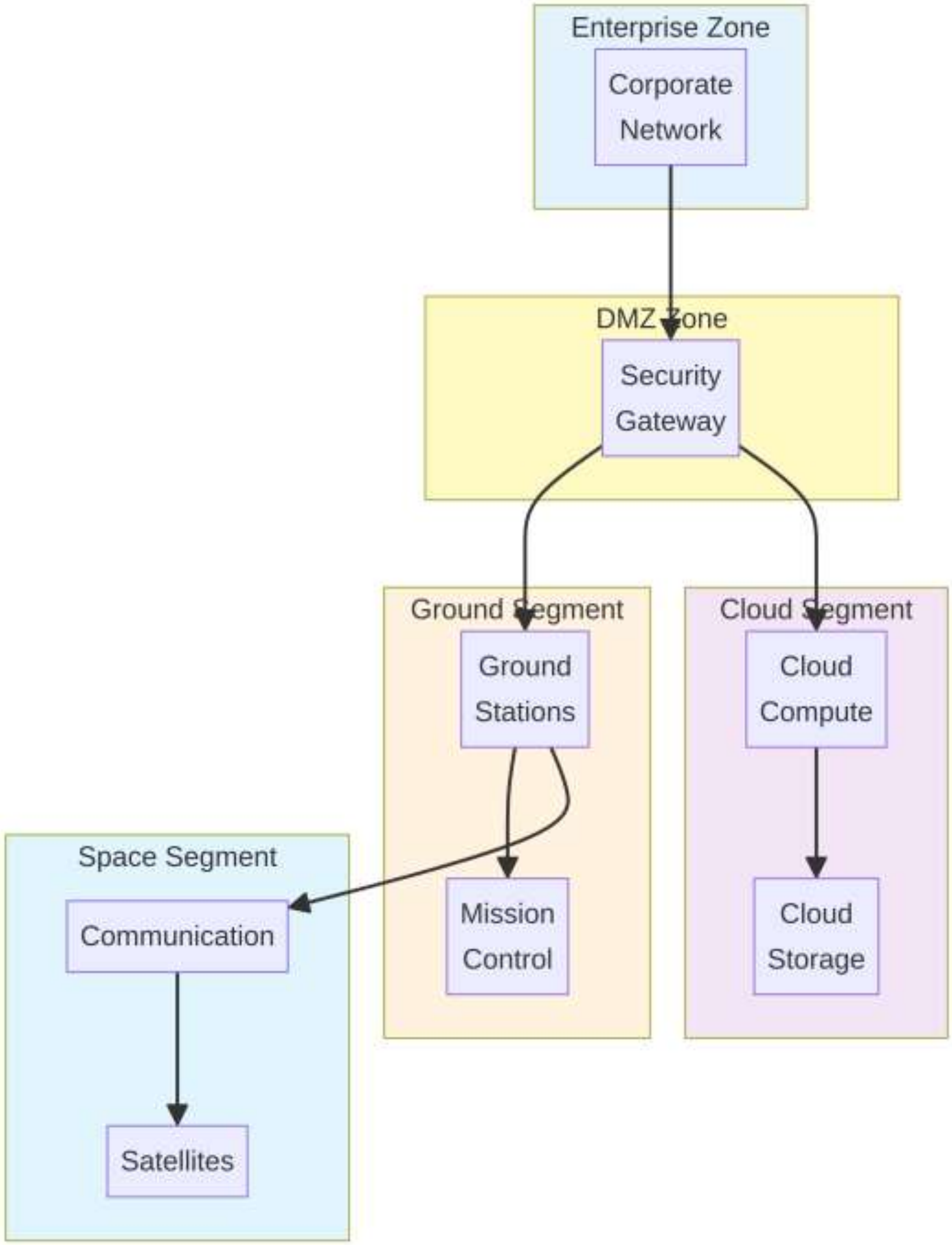

Figure 3: Adapted Purdue Model for Space Systems

4. RESEARCH DESIGN AND METHODOLOGY

This study employs a qualitative, descriptive research methodology based on a systematic literature review. The research process was designed to synthesize existing knowledge on cloud computing security for space operations and to identify the key challenges, existing solutions, and future research directions. The methodology was executed in three distinct phases:

1. **Literature Scoping and Collection:** The first phase involved a comprehensive search for relevant academic and industry publications. The search was conducted across multiple databases, including IEEE Xplore, ACM Digital Library, and Google Scholar. The search queries included a combination of keywords such as "cloud computing," "space security," "cybersecurity," "satellite communication," "threat mitigation," and "access control." The inclusion criteria for the literature were: (a) relevance to the intersection of cloud computing and space security; (b) publication in a peer-reviewed journal or a reputable conference; and (c) publication within the last ten years to ensure the currency of the information. A total of 78 articles were initially identified, which were then screened for their direct relevance to the research questions.
2. **Content Analysis and Synthesis:** The second phase involved a detailed analysis of the selected literature. The content of each article was systematically reviewed to extract key information related to the research questions. This included identifying the main arguments, the methodologies used, the key findings, and the limitations of each study. The extracted information was then synthesized to build a comprehensive understanding of the current state of the field. This process of synthesis was guided by the conceptual framework of this study, which focuses on the pillars of threat mitigation and access control.
3. **Framework Development and Critical Review:** The final phase of the methodology involved the development of a conceptual framework for securing space-cloud systems. This framework was derived from the synthesis of the literature and is intended to provide a holistic and integrated approach to space-cloud security. The framework was then used as a basis for a critical review of the existing security paradigms and for identifying the remaining gaps in the literature. This critical review forms the basis of the discussion and conclusion sections of this article.

This qualitative and descriptive approach was chosen because it is well-suited for exploring a complex and rapidly evolving field like space-cloud security. It allows for a nuanced and in-depth analysis of the existing literature and provides a solid foundation for the development of new theoretical insights.

5. FINDINGS AND DISCUSSION

The systematic review of the literature reveals a growing body of research at the intersection of cloud computing and space security. However, the field is still in its nascent stages, and there are several significant gaps in the existing knowledge. This section discusses the key findings of this study, focusing on the challenges of adapting terrestrial security models to the space environment, the critical role of threat mitigation and access control, and the potential of Zero Trust Architecture (ZTA) to address the unique security challenges of space-cloud systems.

5.1. The Challenge of Adapting Terrestrial Security Models

One of the central findings of this study is that the direct application of terrestrial security models to the space environment is often inadequate. The unique characteristics of space operations—such as high latency, intermittent connectivity, and the physical inaccessibility of assets—pose significant challenges for traditional security paradigms. For example, the high latency of space-to-ground communications can render real-time threat detection and response mechanisms ineffective. Similarly, the limited bandwidth of satellite links can make it difficult to implement data-intensive security measures, such as continuous monitoring and logging. The UK government's 2025 report on cyber risks of cloud computing in the ground segment of the space sector confirms these challenges, noting that cloud integration expands the attack surface while introducing new operational technology (OT) security concerns [25].

Furthermore, the multi-tenant nature of cloud computing introduces a new layer of complexity. In a shared infrastructure, it is essential to ensure that the actions of one user do not compromise the security of others. This is particularly challenging in the context of space operations, where multiple government agencies and commercial entities may be sharing the same cloud resources through Ground Station as a Service (GSaaS) models. The shared responsibility model in cloud services requires clear delineation of security obligations between GSaaS providers and users to prevent accountability gaps. Legacy systems pose an additional challenge, as many satellite systems were not designed with modern cybersecurity practices in mind. Integrating these systems with cloud-based solutions requires careful consideration to avoid exposing outdated interfaces and insecure protocols [25]. The literature suggests that a new generation of space-tailored security solutions is needed to address these challenges. These solutions must be lightweight, resilient, and adaptable to the unique constraints of the space environment.

Figure
Figure 4: Security Challenges and Mitigation Strategies

5.2. The Centrality of Threat Mitigation and Access Control

This study confirms that threat mitigation and access control are the two fundamental pillars of any effective space-cloud security architecture. The literature is replete with examples of how failures in these two areas can lead to catastrophic consequences. The 2022 ViaSat incident, for instance, was a stark reminder of the importance of robust threat mitigation. The attack, which was attributed to a lack of proper network segmentation and weak access controls, resulted in the disruption of satellite services across Europe and had a significant impact on the conflict in Ukraine [3]. Recent research by Khan et al. (2024) has comprehensively documented the spectrum of space cyber-attack vectors, encompassing the ground, space, user, cloud, communication channels, and supply chain segments, and has evaluated the effectiveness of legacy security controls in addressing these threats [26].

The findings of this study also highlight the need for a more proactive and intelligence-driven approach to threat mitigation. The traditional, reactive approach to security is no longer sufficient in the face of sophisticated and well-funded adversaries. Instead, space operators must leverage real-time threat intelligence, predictive analytics, and AI-driven tools to anticipate and neutralize threats before they can cause harm. This includes implementing robust supply chain security practices, as malicious firmware and legitimate update exploitation have been documented as attack vectors in space systems [22]. Similarly, access control mechanisms must be dynamic and context-aware, taking into account factors such as user behavior, device health, and the sensitivity of the data being requested. The principle of least privilege must be rigorously enforced to minimize the impact of insider threats and unauthorized access, particularly in environments where a single misused privilege could compromise sensitive mission data or disrupt critical operations [27].

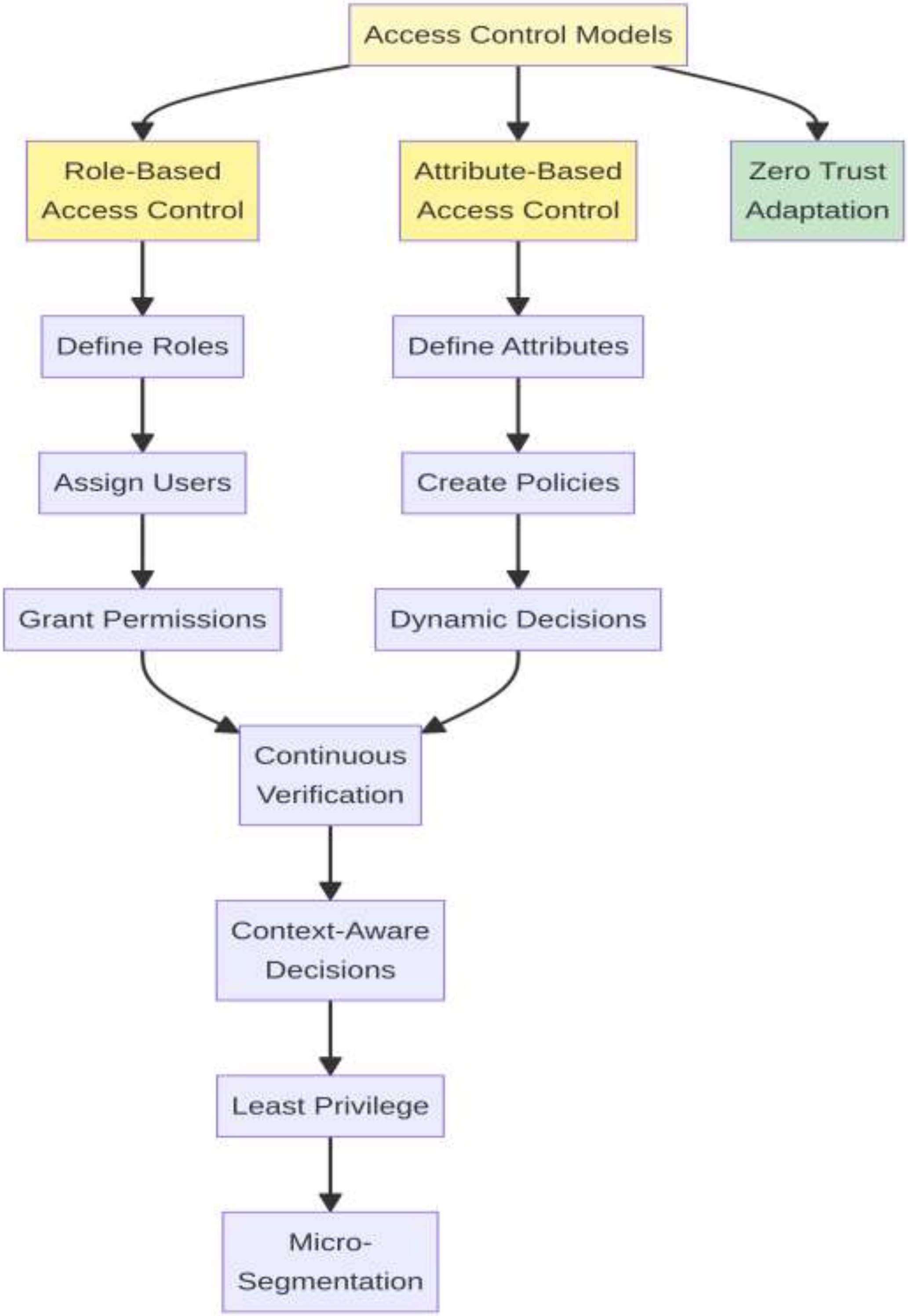

Figure 5: Access Control Models Comparison

5.3. The Promise of Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) is emerging as a promising solution to many of the security challenges facing space-cloud systems. By operating on the principle of "never trust, always verify," ZTA can significantly reduce the attack surface and mitigate the risk of unauthorized access. The literature suggests that ZTA is particularly well-suited to the distributed and heterogeneous nature of space-cloud environments, where the traditional network perimeter is becoming increasingly blurred [18]. The CISA report on Space Systems Security and Resilience Landscape (2024) provides comprehensive guidance on implementing ZTA in space environments, addressing both the technical and organizational aspects of this transition [23].

Practical implementations of ZTA in space systems are beginning to emerge. The FORTRESS framework, for example, demonstrates how kernel-level runtime security through KubeArmor can be integrated with workload identity management using SPIFFE to enforce zero trust principles in containerized satellite systems [24]. This approach is particularly relevant for modern satellite constellations, especially in Low Earth Orbit (LEO), which increasingly rely on containerized payloads and microservice-heavy architectures. By enforcing fine-grained policies at the system-call level and ensuring continuous validation during all phases of the software lifecycle, FORTRESS addresses the unique security requirements of space-edge systems.

However, the implementation of ZTA in the space domain is not without its challenges. The high latency and intermittent connectivity of satellite links can make it difficult to implement the continuous verification and dynamic access controls that are at the heart of the ZTA model. Furthermore, the resource-constrained nature of many space systems can make it challenging to deploy the sophisticated monitoring and analytics tools that are required for effective ZTA. Despite these challenges, the potential benefits of ZTA are significant, and it is likely to become a key component of any future-proof space-cloud security architecture, particularly as satellite systems become increasingly autonomous and require self-healing security mechanisms during periods of disconnection.

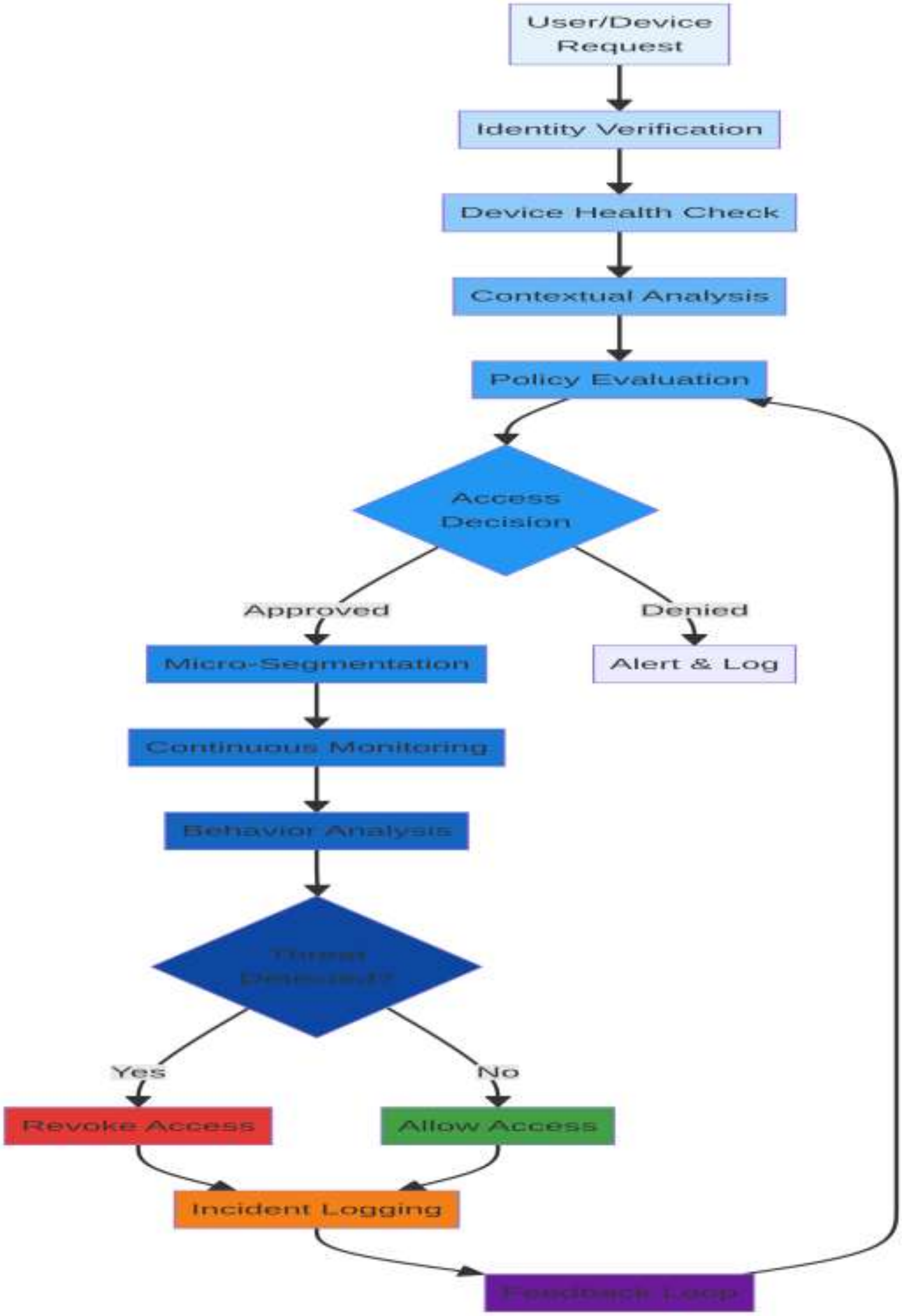

Figure 6: Zero Trust Architecture Implementation Flow

6. Contribution to Knowledge

This article makes several significant contributions to the existing body of knowledge on cloud computing security for space operations. These contributions are threefold:

1. **A Synthesized and Critical Review of the Literature:** This study provides one of the first comprehensive reviews of the academic and industry literature at the intersection of cloud computing and space security. By synthesizing the findings of numerous disparate studies, this article provides a holistic and up-to-date overview of the current state of the field. The critical nature of this review also helps to identify the key gaps in the existing literature, thereby providing a roadmap for future research.
2. **A Conceptual Framework for Space-Cloud Security:** This article proposes a conceptual framework for securing space-cloud systems that is built upon the two fundamental pillars of threat mitigation and access control. This framework is designed to be both comprehensive and adaptable, and it can be used by space operators to design and implement more resilient security architectures. The framework also incorporates the emerging paradigm of Zero Trust Architecture (ZTA), which is likely to become a key component of any future-proof space-cloud security strategy.
3. **Actionable Recommendations for Industry and Government:** The findings of this study have significant practical implications for both industry and government. The article provides a set of actionable recommendations for developing and implementing more effective space-cloud security solutions. These recommendations are grounded in the latest academic research and industry best practices, and they can be used to inform the development of new security policies, standards, and technologies.

In summary, this article provides a timely and much-needed contribution to a rapidly evolving field. By bridging the gap between the academic discourse on cloud security and the practical challenges of space operations, this study provides a valuable resource for researchers, practitioners, and policymakers alike.

7. Recommendations for Future Work

Based on the findings of this study, several recommendations emerge for both the research community and industry practitioners:

For Researchers: Future studies should focus on developing and testing advanced technological solutions that address the unique constraints of space environments. This includes research on lightweight encryption algorithms suitable for high-latency communications, adaptive anomaly detection systems that can function with intermittent connectivity, and autonomous security mechanisms for satellites during periods of disconnection from ground control.

For Industry: Space operators and cloud service providers should prioritize the implementation of Zero Trust Architecture principles in their systems. This includes conducting threat modeling and red teaming exercises specific to space-cloud environments, establishing clear security responsibilities in GSaaS contracts, and investing in security certification schemes and training programs for personnel across the supply chain.

For Policymakers: Governments should develop international standards and policies for space cybersecurity that account for the unique characteristics of the space domain. This includes fostering stakeholder collaboration, supporting smaller operators in the space supply chain with cybersecurity resources and expertise, and establishing frameworks for information sharing regarding space-related cyber incidents.

8. CONCLUSION

The integration of cloud computing into space operations represents a pivotal advancement, offering unprecedented capabilities for data management and mission flexibility. However, this evolution is not without its perils. The expanded attack surface and the increasing sophistication of cyber threats have made the security of space-cloud systems a matter of urgent international concern. This article has provided a critical review of the current state of space-cloud security, focusing on the foundational pillars of threat mitigation and access control.

The findings of this study underscore the inadequacy of directly applying terrestrial security models to the unique and challenging environment of space. The high latency, limited bandwidth, and physical inaccessibility of space assets demand a new generation of lightweight, resilient, and adaptable security solutions. The principles of proactive threat mitigation and granular access control, as outlined in this article, provide a solid foundation for the development of these solutions. Furthermore, the emergence of Zero Trust Architecture (ZTA) offers a promising path forward, although its implementation in the space domain will require innovative solutions to overcome the inherent challenges of the environment.

As we venture further into this new era of space exploration and commercialization, the security of our space-based assets will be of paramount importance. The continued development of robust, space-tailored security frameworks is not merely a technical imperative but a strategic necessity. It is our hope that this article will serve as a valuable resource for researchers, practitioners, and policymakers as they work to secure the final frontier.

REFERENCES

[1] S. K. Ramesh Naidu, et al., "Cloud-Based Satellite Data Processing and Distribution: A Review," Journal of Big Data, 2021.

[2] A. Abbas, et al., "A Survey on Security and Privacy Issues in Cloud-Based E-Health Systems," Journal of Network and Computer Applications, 2021.

[3] ENISA, "ENISA Threat Landscape for 5G Networks," ENISA Reports, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks-1

[4] U.S. Government Accountability Office (GAO), "High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas," GAO-19-157SP, 2020.

[5] NASA Office of Inspector General, "NASA's Cybersecurity Readiness," IG-21-013, 2021.

[6] M. Manulis, et al., "A Survey of Security and Privacy in Satellite-Based Communication Systems," IEEE Communications Surveys & Tutorials, 2021.

[7] T. Tatineni, "A Comprehensive Review of Cybersecurity in Critical Infrastructure," International Journal of Critical Infrastructure Protection, 2023.

[8] M. Ali, et al., "A survey on security issues and solutions in cloud computing," Journal of Network and Computer Applications, vol. 57, pp. 12-32, 2015.

[9] N. Amara, et al., "Cloud computing security threats and attacks with their mitigation techniques," in 2017 International Conference on Engineering & MIS (ICEMIS), 2017.

[10] A. Pauley, et al., "Cybersecurity in the New Space Age: A Survey of Threats and Countermeasures," IEEE Aerospace and Electronic Systems Magazine, 2022.

[11] V. Mavroeidis, et al., "A Survey of Threat Intelligence Platforms," Journal of Cybersecurity and Privacy, 2021.

[12] Y. Chen, et al., "A Hierarchical Approach for Cybersecurity Risk Assessment in Industrial Control Systems," IEEE Transactions on Industrial Informatics, 2022.

[13] A. Ahmed, et al., "A Review on Encryption and Authentication Techniques for Secure Communication," Journal of Information Security and Applications, 2023.

[14] L. Atzori, et al., "A survey on using machine learning for anomaly detection in industrial networks," IEEE Communications Surveys & Tutorials, 2021.

[15] V. Nnamoko, et al., "A Survey of Multi-Factor Authentication Schemes," Journal of Information Security and Applications, 2022.

[16] S. Choudhary, "A Comparative Study of Access Control Models for Cloud Computing," International Journal of Computer Applications, 2023.

[17] N. Sidharth, "The Principle of Least Privilege: A Cornerstone of Modern Cybersecurity," Cybersecurity Today, 2022.

[18] R. Fernandez & A. Brazhuk, "Zero Trust Architecture: A Comprehensive Review," ACM Computing Surveys, 2023.

[19] K. Phiayura & S. Teerakanok, "A Systematic Review of Zero Trust Architecture Implementation and Challenges," IEEE Access, 2023.

[20] AccuKnox, "Space Satellite Cyber Security: Zero Trust Framework with AccuKnox FORTRESS," AccuKnox Blog, November 2025. [Online]. Available: https://accuknox.com/blog/space-satellite-cyber-security
[21] Ibid.
[22] Ibid.
[23] Cybersecurity and Infrastructure Security Agency (CISA), "Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment," CISA Reports, April 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-06/Space%20Systems%20Security%20and%20Resilience%20Landscape%20-%20Zero%20Trust%20in%20the%20Space%20Environment%20%28508%29.pdf
[24] AccuKnox, "Space Satellite Cyber Security: Zero Trust Framework with AccuKnox FORTRESS," AccuKnox Blog, November 2025. [Online]. Available: https://accuknox.com/blog/space-satellite-cyber-security
[25] UK Department for Science, Innovation & Technology, "Cyber risks of cloud computing in the ground segment of the space sector," Government Publications, August 2025. [Online]. Available: https://www.gov.uk/government/publications/cyber-risks-of-cloud-computing-in-the-ground-segment-of-the-space-sector
[26] S. K. Khan, et al., "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions," International Journal of Critical Infrastructure Protection, vol. 47, 2024.
[27] N. Kodakandla, "The Principle of Least Privilege in Space-Cloud Environments," Journal of Space Security, 2025.

Appendix A: Summary of Key Security Challenges and Mitigation Strategies

The following table provides a comprehensive overview of the primary security challenges identified in space-cloud environments and their corresponding mitigation strategies:

Security Challenge	Description	Mitigation Strategy
****Expanded Attack Surface****	The integration of cloud services and ground stations expands the potential entry points for cyberattacks.	Implement Zero Trust Architecture (ZTA) to enforce strict access controls and continuous verification.
****Supply Chain Vulnerabilities****	Malicious code or vulnerabilities can be introduced through third-party software and hardware components.	Enforce rigorous supply chain security practices, including code scanning and vendor security assessments.
****Legacy System Integration****	Integrating older satellite systems with modern cloud infrastructure can expose insecure protocols and interfaces.	Isolate legacy systems using network segmentation and apply compensating controls to protect them.
****High Latency and Intermittent Connectivity****	The space environment poses challenges for real-time security monitoring and response.	Deploy autonomous, on-board security solutions that can operate during periods of disconnection from ground control.
****Insider Threats****	Malicious or negligent insiders with privileged access can cause significant damage.	Enforce the principle of least privilege, implement robust access controls, and monitor user activity for anomalies.
****Data Breaches****	The vast amounts of data generated by space missions are attractive targets for theft and espionage.	Utilize end-to-end encryption for data in transit and at rest, and implement strong access control policies.
****Denial-of-Service (DoS) Attacks****	Attacks can disrupt communication links and render satellite services unavailable.	Implement DoS mitigation techniques, such as traffic filtering and rate limiting, and ensure network redundancy.
****Ransomware and Malware****	Destructive malware, such as AcidRain, and ransomware can disable critical systems and hold data hostage.	Employ advanced malware detection and prevention systems, and maintain regular backups of critical data.

This table synthesizes the key findings from the literature review and provides practitioners with a quick reference guide for addressing the most critical security challenges in space-cloud environments.