International Journal of Emerging Engineering and Technology (IJEET)
ISSN (e): 2958-3764
Volume: 4, Number: 2, Pages: 44 - 51, Year: 2025

AI-Driven Cybersecurity for Satellite Systems: A Survey of Threats, Applications, Challenges and Future Directions

Sania Khan [1,*], Irshad Ahmed Sumra [1], and Makhdoom Zain Ul Abdin [2]

[1,] Department of Informatics and Systems, University of Management and Technology, Lahore, 54000, Pakistan
[2] Department of Pharmacy, University of Karachi, Karachi, 74000, Pakistan
[*] Corresponding author: Sania Khan (Email: f2025375004@umt.edu.pk)

***Abstract*—Satellite systems have become increasingly important for communication, navigation, defence, emergency management, Earth observation, finance, and other critical infrastructure services. These systems are increasingly connected to ground stations, cloud platforms, Commercial Off-the-Shelf (COTS) systems, open-source software, and Artificial Intelligence (AI) and autonomous systems, thereby increasing their cyberattack surface. This survey explores the threats, applications, challenges, and future directions of AI in satellite-based cybersecurity in this survey. It highlights two recent studies, one of which combines Quantum Key Distribution (QKD) with CatBoost Machine Learning (ML) for secure satellite communications, and the other of which is a taxonomy of cyber vulnerabilities, spanning legacy, operational, and AI-enabled space systems. The review concludes that AI can be used for anomaly detection, threat classification, risk prioritisation and decision support, and quantum cryptography can enhance key exchange. To ensure future progress, there is a need for explainable AI and resilient security frameworks.**

***Index Terms*— AI-driven cybersecurity, anomaly detection, CatBoost, cyber vulnerabilities, Quantum cryptography, Satellite cybersecurity, space systems.**

I. INTRODUCTION

Satellite systems are an integral part of physical and digital infrastructure in the modern world [1]. They are used in communication, navigation, Earth observation, defence operations, emergency response, financial services, agriculture, energy systems, and environmental monitoring. These services are linked to both national security and civilian life, and the disruption of satellite systems can have serious repercussions. Breaking into a satellite, ground station, or command line could disrupt military communications, GPS, disaster response, aviation, banking transactions, or critical infrastructure operations. Space-based assets are now increasingly intertwined with terrestrial infrastructure, and cyber threats to space include data exfiltration, spoofing, malware attacks, signal jamming and attacks on ground control systems [2].

The complexity of satellite cybersecurity is growing, as modern space systems are neither isolated nor purely hardware-based [3]. They are increasingly reliant on commercially available off-the-shelf components, open source software, cloud-based services, artificial intelligence, Internet of Things devices, and autonomous decision-making technologies. All these developments add efficiency and flexibility, but also increase the attack surface. Weak software reliance, insecure cloud systems, corrupt supply chains, and inadequately tested AI models are just a handful of factors that can create new avenues for attacks. AI systems in space also pose new challenges, such as data poisoning, black-box decision-making, false anomaly detection, and unsafe autonomy control decisions, as highlighted by [2].

Another major issue is the future vulnerability of conventional cryptographic systems. Satellite communications are typically secured using classical encryption techniques, which could become less reliable in the future with the advent of quantum computing. Authors in [1] state that there are already significant security and operational issues with satellite communication systems, such as signal interception, jamming, long-distance delay, privacy breaches, and interference. To solve these problems, they suggest using satellite communication security and threat -evel prediction based on a combination of quantum cryptography and machine learning (CatBoost) [4].

Thus, AI-based cybersecurity in satellite systems is a key and timely research field. Protecting only the satellite is insufficient; the complete satellite system (space segment, ground segment, command links, software supply chain, cloud services, cryptographic systems, and autonomy via AI systems) should be taken into consideration [5]. The goal of this survey paper is to compare two recent papers published

in 2025 and 2026 and to examine how artificial intelligence, quantum cryptography, and the taxonomy of cyber vulnerabilities can be used to enhance the security of satellites.

The rest of this paper is organised as follows. Section II explains the survey methodology and paper selection process. Section III reviews literature on AI, quantum cryptography, anomaly detection, and satellite cyber vulnerabilities. Section IV compares the selected studies in terms of methods, applications, findings, and limitations. Section V discusses research gaps and future directions. Section VI concludes the paper with the main findings and recommendations.

II. SURVEY METHODOLOGY

In this study, the methodology being used is a review-based survey method, not an experimental method, as shown in Fig. 1. The goal is not to gather primary data nor test a new model, but to critically review and compare two recent journal papers on the subject of cybersecurity for satellite and space systems in the context of AI. Supporting studies were used to broaden the review across anomaly detection, QKD, GNSS interference, satellite communication security, adversarial AI, and COTS/cloud/supply-chain risks. The first paper selected is [1], on Security in Satellite Communication using Quantum Network and CatBoost machine learning. This paper is technical and model-based, as it covers QKD, machine-learning-based threat classification, and the prioritisation of security features in satellite communication systems [5].

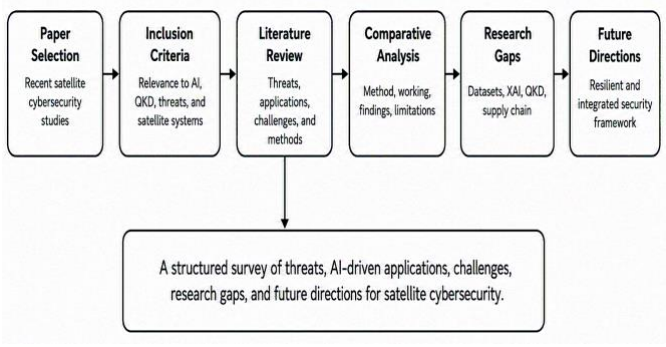

Fig. 1. Survey methodology

The second paper is authored by [2] and addresses the need to build a taxonomy for cyber vulnerabilities in space systems and to present a framework for resilient cyber defense. This paper is more conceptual and framework-oriented, as it identifies weaknesses in legacy systems, operational infrastructure, command pathways, supply chains, space systems with AI, and cloud services.

The novelty of this survey lies in its integrated comparison of AI-driven threat prediction, quantum-secure communication, and space-system vulnerability taxonomy. Existing survey articles often focus separately on satellite communication security, anomaly detection, GNSS interference, or general cyber threats. In contrast, this paper connects three important areas: QKD and CatBoost-based threat prediction, taxonomy-based classification of space-system vulnerabilities, and AI-specific risks such as data poisoning, black-box decision-making, false anomaly detection, and unsafe autonomy. It also highlights practical gaps in real-world datasets, COTS components, cloud infrastructure, supply chain security, and international policy. Therefore, this survey provides a broader and more integrated view of cybersecurity challenges and future directions for next-generation satellite systems. These two papers were chosen because they meet the following criteria:

TABLE I: PAPERS CRITERIA

Criterion	Explanation
Publication year	Both papers are recent, published in 2025 and 2026.
Relevance	Both directly address satellite or space-system cybersecurity.
AI/security focus	Both include AI, machine learning, quantum security, or AI-related cyber risks.
Research value	One paper is technical/model-based, while the other is taxonomy/framework-based.
Suitability for survey	Both allow comparison of threats, methods, applications, challenges, and future directions.

The comparison structure in this survey is based on the handwritten structure idea. The papers are compared based on Author/Year, Proposed Method, Working of the Method, Applications, Key Findings, Limitations, and Future Directions. This framework helps to systematically assess both studies and illustrate how their findings can be utilised for the overall advancement of AI-enabled satellite cybersecurity.

III. LITERATURE REVIEW

A. Quantum Cryptography and ML for Satellite Communication Security

Satellite communication security has come a long way from the days of traditional encryption or standalone network security, as recent studies demonstrate. New defense mechanisms are needed to ensure that transmitted data is protected against interception, jamming, spoofing, privacy violations, and potential attacks by future quantum computers. The authors of [1] address this by proposing a security solution for satellite communication systems that integrates QKD with CatBoost machine learning. Satellite communication faces several long-distance propagation issues, including propagation delay, interference, hacking, privacy violations, and bandwidth constraints, which collectively pose achallengesto ensuring the confidentiality, integrity, and availability of communication [6]. This paper is

crucial to this survey, as it bridges the two key directions of security: quantum-secure communication and AI-driven threat prediction (Fig. 2).

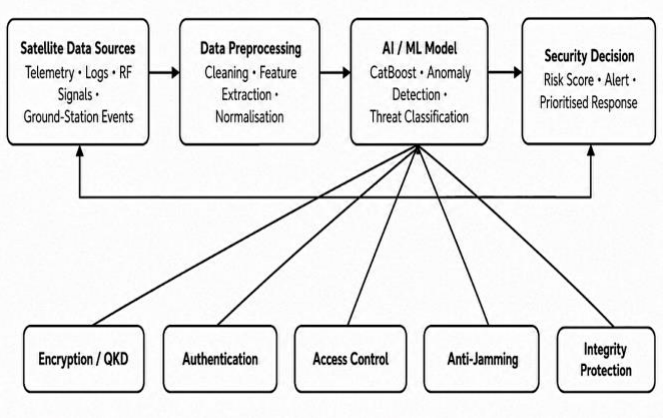

Fig. 2. AI-driven satellite cybersecurity framework integrating data collection.

The authors of [1] have the advantage of considering QKD as a future cryptographic method. QKD differs from traditional cryptographic approaches, which rely on computational difficulty. In contrast to traditional cryptographic techniques, QKD relies on quantum principles to facilitate secure key exchange. This is important in satellite communication because disturbances in the states can signify that the satellite has been compromised [7]. The paper acknowledges, however, that QKD is by no means a straightforward, complete solution. However, there are challenges to address in practical QKD systems, including limited transmission range, implementation costs, infrastructure compatibility, and the need for authenticated classical channels. This balances the paper by not overstating QKD's potential while acknowledging that it remains an early-stage security solution in the satellite environment [8].

The paper's machine learning component uses the CatBoost algorithm, a gradient boosting framework, to process categorical features effectively. It can be used for satellite security, since many security properties are categorical (e.g., encryption type, authentication state, access control, anomaly detection, key management). The authors in [1] employed a synthetic dataset of 10,000 records that encompasses satellite communication security attributes, including encryption, anomaly detection, redundancy and resilience, standards compliance, physical layer security, secure key management, authentication, integrity protection, anti-jamming, and access control [9]. These features enable the model to specify threat levels and determine which controls are most effective at protecting satellite communication.

The major finding of [1] is the high accuracy of 89.23% and AUC-ROC of 94.56% obtained by using the CatBoost model in the experimental setup. Research also revealed that some features, like anomaly detection and quantum encryption, were also crucial in threat prediction. It is important to note that this is not just AI's role in security detection, but also in prioritisation. An AI-based model could also assist satellite operators in prioritising which security controls require greater focus and which threat indicators pose the greatest risk to the system [10]. However, the biggest drawback is that the dataset is synthetic. Thus, the results should not be considered definitive in actual use. The model would have to be validated in operational conditions with real satellite telemetry, attack traces, jamming data, and ground-station logs.

Other research supports the need for AI-based anomaly detection in space environments. As noted in [5], space information networks face specific anomaly detection challenges, including scalability, real-time detection, limited labelled data, concept drift, and adversarial attacks. The issues are relevant because satellite systems produce dynamic, distributed data, and an attacker can attempt to manipulate traffic or telemetry to evade detection. Likewise, [10] discuss the security challenges of space information networks, as well as secure routing and anomaly detection, from both traditional and AI perspectives. Their research backs up the thesis that AI is increasingly playing a pivotal role in space-network defence, particularly when rule-based detection proves inadequate [11].

AI-driven satellite cybersecurity has also recently made strides toward federated and privacy-preserving detection. In their paper, [7] present a federated framework for anomaly detection in satellite networks that incorporates both intelligent client selection and deep learning. The relevance is that satellite networks are distributed, and federated learning may help train models without centralising sensitive operational data [12]. While federated learning brings its own set of challenges, including model poisoning, communication overhead, and unreliable client behaviour, its ability to leverage a decentralised edge AI network for distributed data shows great promise. Thus, the accuracy of AI-based satellite cybersecurity is not the only criterion to consider; resilience, interpretability, and operational feasibility also need to be considered [13]. The studies indicate that there is technical potential for QKD, but mission-level planning is needed for deployment [14]. Space systems consist of ground stations, command pathways, onboard systems, software dependencies, cloud platforms, commercial components, supply chains, and, more than ever, AI autonomy [15].

Both [1] and [2] provide technical models for AI and quantum security, but Dawson and Khan's taxonomy of cyber vulnerabilities for space systems is a broader framework. Their paper is noteworthy because the only way to understand satellite cybersecurity is not to look at communication encryption or threat classification. According to [2], space-based assets are used for communication, navigation, surveillance, defence, and critical infrastructure, which makes them attractive targets for exploitation through cyber means.

They classify vulnerabilities into three broad categories: Legacy Systems, Operational Infrastructure, and AI-enabled Systems. Weaknesses in the ground and space segments are among the legacy system risks. The ground segment is of particular importance, as the attacker may exploit access points to the system to send unauthorised commands or extract information [16]. The space segment consists of

telemetry, tracking, and Command systems, avionic components, and onboard data handling systems that can be subject to intrusion or hijacking. The operational infrastructure risks are weak command links, compromised supply chain, COTS components, open-source software, cloud-based infrastructure, and onboard IoT devices. Data poisoning, unclear AI model design, erroneous anomaly detection, and unsafe AI decision-making are all risks in the context of AI [17]. The satellite threats should be analysed from the entire system architecture and are summarised in an extensive survey by [3], which details satellite communication cybersecurity in the space, ground, and link segments. The attacks and defences on satellite communication can also be categorised by [4] based on the three elements of the cybersecurity framework: confidentiality, integrity, and availability, which helps organise the security risks in satellite communication within a clear cybersecurity structure. Sharmin et al. [6] also resume cyber threats to space information networks and divide them into active and passive threats, offering practical examples of attacks, such as DoS attacks and message manipulation [18].

The authors in [1] focus on quantum-secure satellite communication, which is also propelled by research in QKD. Satellite platforms are also suitable for long-distance quantum communication, as demonstrated by [19], who achieved entanglement over a distance of more than 1200 km. Also, [20] applied the QKD protocol to the photon loss during ground propagation to the satellite, as well as to the processing time limits, which is useful for understanding practical limitations in satellite QKD. Cyber Vulnerability Taxonomy for Space Systems by broader arguments in satellite cybersecurity shown in Fig. 3.

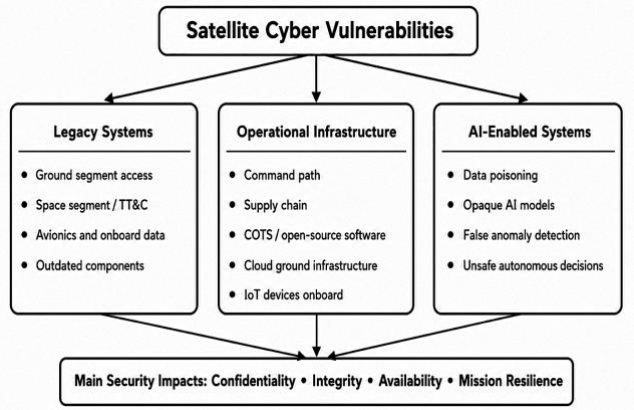

Fig. 3. Taxonomy of satellite cyber vulnerabilities

One of the strengths of [2] is the link that they draw between incidents and their taxonomy in the real world, such as NASA cyber breaches, GPS interference in Europe, and satellite hijacking attempts. This makes the paper of some practical use, since it does not just treat satellite cybersecurity as a theoretical concern. The drawback is that it is mostly conceptual and framework-oriented. Does not adopt or evaluate a technical model for AI detection. Future research should therefore integrate the best of both worlds in [2] with other model-based techniques, such as the CatBoost framework, which has proven effective. The entire AI-based satellite cybersecurity architecture should address vulnerabilities across ground, space, command, cloud, supply chain, and AI systems, and incorporate existing machine learning models that have been validated and trained on real operational data [19].

IV. COMPARATIVE ANALYSIS

A comparative analysis of the selected studies in terms of the methodology, working mechanism, application, main conclusions, and limitations is presented, along with recommendations for future research. As the comparison demonstrates, AI-driven cybersecurity for satellite systems cannot be viewed from a single perspective. Some of the studies are technical security models (e.g., machine learning, quantum cryptography, and anomaly detection), while othersfocuse on vulnerability mapping, policy frameworks, and cyber resilience at the system level [20]. Thus, the comparative analysis assists in identifying the contributions of different approaches to the protection of satellite communication systems, ground stations, command pathways, and space infrastructure using AI capabilities.

TABLE II
COMPARATIVE ANALYSIS OF SELECTED STUDIES ON AI-DRIVEN SATELLITE CYBERSECURITY

Author(s) / Year	Proposed Method	Working of Method	Applications	Key Findings	Limitations
[1]	Quantum cryptography integrated with CatBoost machine learning	Uses QKD for secure key exchange and CatBoost ML for classifying threat levels using satellite communication security features	Secure satellite communication, threat prediction, anomaly detection, encryption selection, and security prioritisation	CatBoost achieved 89.23% accuracy and 94.56% AUC-ROC. Anomaly detection and quantum encryption were highly important features	Uses a synthetic dataset; practical QKD deployment is costly and faces range and infrastructure limitations
[2]	Cyber vulnerability taxonomy and resilient infrastructure framework	Classifies vulnerabilities across legacy systems, operational infrastructure, command pathways, supply chains, cloud services, COTS compone	Space-system risk assessment, cyber resilience planning, policy development, and infrastructure protection	Identifies ground segment, command link, supply chain, cloud, COTS, and AI-related vulnerabilities such as data poisoning and black-box models	Mainly conceptual; does not test an AI detection model or validate the framework using real satellite datasets

		nts, and AI-enabled systems			
[5]	Survey of anomaly detection for space information networks	Reviews AI and machine learning methods for detecting abnormal patterns in space network traffic and system behaviour	Real-time anomaly detection, intrusion detection, network monitoring, and early warning systems	Highlights major challenges such as limited labelled data, scalability, concept drift, adversarial attacks, and real-time detection requirements	Survey-based study; practical implementation and real-world validation remain limited
[3]	Comprehensive survey of satellite communication cybersecurity	Reviews threats, vulnerabilities, and countermeasures across the space, ground, and communication-link segments	Satellite communication protection, architecture-level security planning, and defence strategy development	Shows that satellite cybersecurity must be addressed across the full system architecture rather than focusing only on one component	Broad survey; less emphasis on testing specific AI or ML models in operational satellite environments
[4]	CIA-based classification of satellite communication attacks and defences	Organises attacks and security controls according to confidentiality, integrity, and availability principles	Threat classification, security control mapping, and satellite communication defence planning	Provides a clear cybersecurity structure for understanding satellite communication risks and countermeasures	Does not deeply examine AI-specific vulnerabilities such as data poisoning or autonomous decision errors

The comparison reveals that the study by [1] contributes the most technically and is the most model-based among the selected studies. Their work is useful because it merges quantum cryptography and machine learning and demonstrates how CatBoost can be used to forecast the threat level to communication from satellites [21]. This method is beneficial for proactive cybersecurity, as it can not only detect threats after they occur but also aid in prioritising security features such as anomaly detection, encryption, authentication, access control, anti-jamming, and secure key management. The results achieved in the study indicate that machine learning could be a valuable tool for threat classification and decision-making in satellite security, with high accuracy and an AUC-ROC score. The main drawback, however, is that the dataset is synthetic and may not be fully representative of the satellite's real operating environment [22]. It would require telemetry data, ground-station locations, jamming incidents, spoofing attacks, and attack traces for real-world testing and validation if this method were used in an operational setting.

The authors of [2], however, offer a more comprehensive and strategic contribution. Their taxonomy is helpful because it reveals that satellite cybersecurity does not have to rely on encrypted links for communication. Rather, weaknesses can manifest within the ground segment, space segment, command lines, supply chains, COTS components, open-source software, cloud infrastructure, IoT devices and AI-based autonomous systems. This broader perspective is critical as a satellite mission might be put at risk even if the communication link itself is secure, due to a breach of some part of the ground infrastructure or software, or through exploitation of a compromised component of the supply chain [23]. A key strength of the study is that it incorporates vulnerabilities unique to AI, including data poisoning, the vagueness of AI model design, false anomaly detection and unsafe autonomous decisions. However, one of its drawbacks is that it is not implemented or tested with a detection model.

The supporting studies reinforce the comparison with the technical detection approach and the architecture-level risk analysis needed for satellite cybersecurity. In this context, [5] state that with the increasing amount of dynamic and distributed data generated by modern space systems, anomaly detection becomes crucial for space information networks. Their work backs up the thesis that AI can be used to help uncover abnormal behaviour, but it also demonstrates that a lack of labelled datasets, concept drift, scalability and adversarial attacks are all significant challenges [24]. Likewise, [3] and [4] demonstrate that the satellite cybersecurity domain should be explored across the entire space, ground, and link architecture in the context of well-known cybersecurity principles such as confidentiality, integrity, and availability.

In conclusion, the comparative study suggests a future trend where AI-powered satellite cybersecurity will integrate the best elements of both technical and conceptual strategies. Model-based studies, such as [1], can be useful for automated threat prediction and security prioritisation, and taxonomy-based studies, e.g., [2], can be helpful in identifying vulnerability focus areas throughout the satellite ecosystem. A more robust future framework would include both and would leverage a taxonomy of vulnerabilities to map attack surfaces and validated AI models to detect, classify, and respond to threats in real time [25]. This integrated solution would offer enhanced defence for satellite communications, mission operations, ground infrastructure, and autonomous space systems with AI capabilities.

V. RESEARCH GAPS AND FUTURE DIRECTIONS

Based on the literature reviewed, AI-based cybersecurity

for satellite systems is progressing rapidly, yet significant research gaps remain. Previous research has enhanced knowledge of satellite threats, machine-learning-based anomaly detection systems, quantum cryptography, and a taxonomy of cyber vulnerabilities. However, many of the suggested techniques have yet to be directly applied in actual space-system deployments due to a lack of data, space-system complexities, AI trust concerns, and infrastructure constraints. Thus, future work should shift from theoretical and synthetic experiments to practical, validated and easily explained cybersecurity solutions for satellite systems.

A. Lack of Real-World Satellite Cybersecurity Datasets

One of the key research gaps is the scarcity of cybersecurity datasets from the real world that are accessible for satellite applications. Most of the AI research is based on synthetic data, simulated network traffic, or general cybersecurity datasets, rather than on actual data from satellite telemetry, ground stations, command links, spoofing traces, or jamming events. In this respect, [1] test CatBoost on a synthetic dataset of 10k records for threat-level prediction. Even though the accuracy and AUC-ROC performance are promising, the results were reported on synthetic datasets, which may not fully represent real operational satellite conditions. The harshness of real satellite environments, including noise, latency, atmospheric effects, hardware constraints, communication patterns unique to the mission, and hostile behaviour, may not be easily replicated in synthetic data [26]. Shared benchmark datasets for satellite cybersecurity, while protecting sensitive mission information, should be developed for future studies. The following datasets should contain the following data: telemetry anomaly, loss of communication, access control events, indicators of malware, spoofing attempts, and ground-segment attack traces.

B. Need for Explainable and Trustworthy AI

A significant drawback is the lack of explainability in AI-based satellite cybersecurity models. Communication availability, defence operations, emergency services, navigation, and spacecraft safety are all factors that may be impacted by security decisions for satellite systems and may influence mission-critical functions [27]. So, operators should know why an AI model might categorise a threat as low, medium or high-risk. Black-box AI decision-making is considered a significant vulnerability in AI-based space systems [2]. AI models, by being opaque, could generate false alarms, fail to detect real attacks, or suggest unsafe autonomous actions. Future studies need to be directed towards Explainable Artificial Intelligence (XAI) techniques that can reveal which feature was critical to a decision, for example, indicators of abnormal telemetry, authentication, Quantum Bit Error Rate, access-control violations, or jamming. Explainability will enhance trust, human oversight, auditability and accountability in satellite cybersecurity.

C. Practical Integration of Quantum Security

Satellite communication could be very promising to use quantum cryptography and QKD, but it is not easy. The authors in [1] point out that QKD is a promising future solution for key distribution, and [22] reveal that the design of satellite QKD systems has several key challenges regarding orbit selection, optical link orientation, trusted node, throughput, latency, and implementation expenses. The primary gap is that while many studies explore QKD as a secure solution, fewer focus on integrating it into the current satellite communication infrastructure at scale [28]. Hybrid quantum-classical security frameworks, post-quantum cryptography, key exchange refresh strategies, authenticated classical channels, and cost-effective models for QKD deployment should be explored in future research. This is particularly crucial, since some satellite missions will not be able to afford full QKD infrastructure.

D. Supply-Chain, Cloud, and COTS Security

The use of COTS equipment, open source software, cloud-based services, and outsourcing services is becoming commonplace in modern satellite systems. Such technologies not only reduce costs and increase flexibility but also open up new attack surfaces. The authors in [2] identify significant cyber vulnerabilities in space systems, including supply-chain compromise, COTS components, open-source software, cloud infrastructure, and onboard IoT devices. However, research efforts today remain somewhat limited in applying practical approaches to satellite software supply chain verification, secure update mechanisms, dependency auditing, and the protection of ground stations via the cloud [29]. Secure-by-design Satellite procurement, Software Bill of Materials, Trusted Firmware Updates, Zero-Trust Access Control, Cloud Security Monitoring and Continuous Vulnerability Assessment along the entire Satellite life cycle should all be explored in future work [30].

E. AI-Specific Attacks and Adversarial Resilience

While AI can enhance the security of satellites, AI systems can also be a target for attack. Risks of AI include data poisoning, model design that is hard to understand, false anomaly detection and unsafe autonomous decision-making, as discussed by [2]. These risks are not trivial due to the possibility that adversarial examples, training data manipulation, or changes to model inputs could fool a system. This may cause false confidence, unnecessary alerts, delayed response and unsafe autonomous control decisions in satellite operations [31]. Future studies should thus include adversarial-robust models, secure training pipelines, model integrity checks, the security of federated -learning systems, and the monitoring of AI's behaviour in orbit and on the ground [32].

F. Need for International Standards and Coordinated Policy

Satellite cybersecurity is more than a technical problem; it is a policy and governance problem. Satellites are used by

many international communication, navigation, disaster response, commercial and defence systems. An attack on one satellite system can impact multiple countries and sectors. However, space system cybersecurity, AI safety with autonomous satellites, and cyber incident reporting are in their infancy. International cooperation, shared cybersecurity standards and protocols, satellite incident response, responsible space behaviour, and satellite law and regulation to protect satellite infrastructure are topics that future research should focus on. This is because no single organisation can manage satellite security effectively.

VI. Conclusion

Satellite systems are essential for civilian, commercial, and defence applications, including communication, navigation, Earth observation, disaster management, banking, aircraft communications, agriculture, and energy. Satellite attacks, attacks on ground stations, attacks on command paths, and attacks on communication links are threats to national security, economic activity and public safety due to this dependence. The findings from the literature review indicate that AI-based cybersecurity can enhance protection through anomaly detection, threat classification, threat scoring, behaviour prediction, and prioritising responses. The authors in [1] demonstrate the benefits of QKD and CatBoost machine learning, though experimental tests are required. The weaknesses of legacy systems, supply chains, cloud services, COTS, IoT, and AI autonomy are noted by [2]. Overall, future satellite cybersecurity requires a multi-layered, resilient and integrated approach.

Funding Statement

The authors received no specific funding for this study.

Conflicts of Interest

The authors declare no conflicts of interest to report regarding the present study.

Author Contributions

All authors contributed to the conception, literature review, drafting, and critical revision of this manuscript and approved the final version for submission.

Data Availability Statement

Data is available on reasonable request.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

References

[1] M. Nadeem, S. A. Ansar, S. Halwai, A. Singh, and R. Kumar, "Enhancing data security in satellite communication systems: Integrating quantum cryptography with CatBoost machine learning," Information, vol. 17, no. 3, Art. no. 220, 2026, doi: 10.3390/info17030220.

[2] M. Dawson and A. H. Khan, "Cyber defense of space systems: Taxonomy of vulnerabilities and framework for resilient infrastructure," Land Forces Academy Review, vol. XXX, no. 3(119), pp. 454–465, 2025, doi: 10.2478/raft-2025-0044.

[3] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments," IEEE Communications Surveys & Tutorials, vol. 27, no. 1, pp. 372–425, 2025, doi: 10.1109/COMST.2024.3408277.

[4] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," Sensors, vol. 24, no. 9, Art. no. 2897, 2024, doi: 10.3390/s24092897.

[5] A. A. Diro, S. Kaisar, A. V. Vasilakos, A. Anwar, A. Nasirian, and G. Olani, "Anomaly detection for space information networks: A survey of challenges, techniques, and future directions," Computers & Security, vol. 139, Art. no. 103705, 2024, doi: 10.1016/j.cose.2024.103705.

[6] A. Sharmin, B. U. Mahmud, N. Nabi, M. Shaima, and M. J. H. Faruk, "Cyber attacks on space information networks: Vulnerabilities, threats, and countermeasures for satellite security," Journal of Cybersecurity and Privacy, vol. 5, no. 3, Art. no. 76, 2025, doi: 10.3390/jcp5030076.

[7] B. Wang, J. Xiao, R. Dong, and X. Lyu, "A comprehensive literature review of cybersecurity in satellite networks," Aerospace, vol. 13, no. 3, Art. no. 249, 2026, doi: 10.3390/aerospace13030249.

[8] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," Computer Networks, vol. 216, Art. no. 109246, 2022, doi: 10.1016/j.comnet.2022.109246.

[9] T. Stojnic, A. S. M. Kayes, and W. Rahayu, "A comprehensive literature review of cyber threats and vulnerabilities in IoT-driven satellite networks: Research challenges and future directions," Computer Networks, vol. 272, Art. no. 111678, 2025, doi: 10.1016/j.comnet.2025.111678.

[10] S. K. Khan, N. Shiwakoti, A. Diro, A. Molla, I. Gondal, and M. Warren, "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions," International Journal of Critical Infrastructure Protection, vol. 47, Art. no. 100724, 2024, doi: 10.1016/j.ijcip.2024.100724.

[11] A. Carlo and K. Obergfaell, "Cyber attacks on critical infrastructures and satellite communications," International Journal of Critical Infrastructure Protection, vol. 46, Art. no. 100701, 2024, doi: 10.1016/j.ijcip.2024.100701.

[12] A. Carlo and P. Breda, "Impact of space systems capabilities and their role as critical infrastructure," International Journal of Critical Infrastructure Protection, vol. 45, Art. no. 100680, 2024, doi: 10.1016/j.ijcip.2024.100680.

[13] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in Proc. 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 1–19, doi: 10.1109/SP46215.2023.10351029.

[14] J. Pavur and I. Martinovic, "Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight," Journal of Cybersecurity, vol. 8, no. 1, Art. no. tyac008, 2022, doi: 10.1093/cybsec/tyac008.

[15] C. Van Camp and W. Peeters, "A world without satellite data as a result of a global cyber-attack," Space Policy, vol. 59, Art. no. 101458, 2022, doi: 10.1016/j.spacepol.2021.101458.

[16] P. Breda, R. Markova, A. F. Abdin, D. Jha, A. Carlo, and N. P. Mantı, "Cyber vulnerabilities and risks of AI technologies in space applications," in Proc. 73rd International Astronautical Congress (IAC), Paris, France, 2022.

[17] N. Abdelsalam, S. Al-Kuwari, and A. Erbad, "Physical layer security in satellite communication: State-of-the-art and open problems," IET Communications, vol. 19, no. 1, Art. no. e12830, 2025, doi: 10.1049/cmu2.12830.

[18] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, no. 7670, pp. 43–47, 2017, doi: 10.1038/nature23655.

[19] J. Yin et al., “Satellite-based entanglement distribution over 1200 kilometers,” Science, vol. 356, no. 6343, pp. 1140–1144, 2017, doi: 10.1126/science.aan3211.

[20] J.-P. Bourgoin et al., “Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations,” Physical Review A, vol. 92, no. 5, Art. no. 052339, 2015, doi: 10.1103/PhysRevA.92.052339.

[21] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” npj Quantum Information, vol. 3, Art. no. 30, 2017, doi: 10.1038/s41534-017-0031-5.

[22] D. Orsucci, P. Kleinpaß, J. Meister, I. De Marco, S. Häusler, T. Strang, N. Walenta, and F. Moll, “Assessment of practical satellite quantum key distribution architectures for current and near-future missions,” International Journal of Satellite Communications and Networking, vol. 43, no. 3, pp. 164–192, 2025, doi: 10.1002/sat.1544.

[23] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, “GNSS vulnerabilities and existing solutions: A review of the literature,” IEEE Access, vol. 9, pp. 153960–153976, 2021, doi: 10.1109/ACCESS.2020.2973759.

[24] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente, and E. S. Lohan, “A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 249–291, 2020, doi: 10.1109/COMST.2019.2949178.

[25] Y. Butt, “Effects of Chinese laser ranging on imaging satellites,” Science & Global Security, vol. 17, no. 1, pp. 20–35, 2009, doi: 10.1080/08929880902864376.

[26] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, “CatBoost: Unbiased boosting with categorical features,” in Advances in Neural Information Processing Systems, vol. 31, 2018, pp. 6638–6648.

[27] S. M. Lundberg and S.-I. Lee, “A unified approach to interpreting model predictions,” in Advances in Neural Information Processing Systems, vol. 30, 2017, pp. 4765–4774.

[28] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” in Proc. International Conference on Learning Representations (ICLR), San Diego, CA, USA, 2015.

[29] B. Biggio and F. Roli, “Wild patterns: Ten years after the rise of adversarial machine learning,” Pattern Recognition, vol. 84, pp. 317–331, 2018, doi: 10.1016/j.patcog.2018.07.023.

[30] R. Radhakrishnan, W. W. Edmonson, F. Afghah, R. M. Rodriguez-Osorio, F. Pinto, and S. C. Burleigh, “Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view,” IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2442–2473, 4th Quart., 2016, doi: 10.1109/COMST.2016.2564990 .

[31] Sumra, I.A., Hasbullah, H., Ab Manan, J.-L.: Effects of attackers and attacks on availability requirement in vehicular network: a survey. In: International Conference on Computer and Information Sciences (ICCOINS2014), Malaysia, 3–5 June 2014.

[32] Sumra, I.A., Hasbullah, H.B., AbManan, Jl.B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In: Laouiti, A., Qayyum, A., Mohamad Saad, M. (eds) Vehicular Ad-hoc Networks for Smart Cities. Advances in Intelligent Systems and Computing, vol 306. Springer.