Cybersecurity Challenges in Modern Aviation: Protecting Digital Infrastructure in Aircraft Systems

Saniyah Mariam, Vainavi Swaminathan, Jovita Philix, Dr. Suma S.

Department of CS and IT, Jain University, Bangalore, Karnataka, India

DOI: https://doi.org/10.51584/IJRIAS.2026.110400170

Received: 18 April 2026; Accepted: 24 April 2026; Published: 18 May 2026

ABSTRACT

The rapid digital transformation of the aviation industry has significantly improved operational efficiency, communication, navigation, and passenger services. However, this increasing dependence on interconnected digital systems has also expanded the sector's exposure to cybersecurity threats. Modern aviation relies on aircraft avionics, satellite-based navigation, air traffic management systems, airport information infrastructure, and airline databases, all of which may become targets for cyberattacks.

This paper presents a narrative review of major cybersecurity challenges affecting contemporary civil aviation systems. The study is based on secondary sources including academic literature, regulatory documents, industry reports, and selected incident cases. The review identifies key threats such as GPS spoofing, ADS-B manipulation, malware, ransomware, data breaches, denial-of-service attacks, and insider threats, and examines critical vulnerabilities linked to legacy systems, weak authentication mechanisms, growing system interconnectivity, and fragmented cyber governance.

In addition, the paper examines the main technical and organizational responses discussed in the literature, including intrusion detection systems, continuous monitoring, encryption, zero-trust principles, employee training, and international information-sharing frameworks. The findings suggest that aviation cybersecurity must be approached not only as an information technology issue but also as a broader safety, operational, and regulatory concern requiring coordinated action among airlines, airports, manufacturers, regulators, and cybersecurity experts.

Keywords: Aviation Cybersecurity; Aviation Cyber Threats; GPS Spoofing; ADS-B Vulnerabilities; Intrusion Detection Systems (IDS); Machine Learning; Internet of Things (IoT) in Aviation; Zero Trust Architecture

INTRODUCTION

The integration of conventional aviation systems with contemporary digital technologies has transformed the industry through increased efficiency, safety, and passenger satisfaction. While digital technology has significantly enhanced operational effectiveness, it has simultaneously opened new avenues for risk — most notably, cybersecurity threats. Modern aircraft depend on complex digital systems encompassing avionics, flight control, communication, and onboard entertainment. Ground-based systems such as air traffic control (ATC), airport infrastructure, and airline management platforms similarly rely on complex computer applications and data networks.

The intricacy of these digital networks, combined with the growing adoption of satellite communications and the Internet of Things (IoT), makes aviation a particularly attractive target for cyberattacks. A successful breach in any part of this interconnected ecosystem can result in devastating consequences, ranging from flight safety incidents and operational disruptions to financial losses and erosion of public trust. As threat actors — including cybercriminals, hacktivists, and state-sponsored groups — continue to develop more sophisticated capabilities, the aviation sector faces mounting pressure to understand, anticipate, and respond to evolving cybersecurity challenges.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

This paper presents a structured narrative review of the major cybersecurity challenges facing modern civil aviation. It draws on academic literature, regulatory frameworks, industry publications, and documented incident cases to synthesize current understanding of aviation cyber threats, system vulnerabilities, and mitigation strategies. The review is intended to serve as a comprehensive reference for stakeholders seeking to strengthen cybersecurity posture across the aviation ecosystem.

LITERATURE REVIEW

Overview of Aviation Cybersecurity Research

The growing digitalization of the aviation sector has attracted significant scholarly and institutional attention to cybersecurity risks affecting aircraft systems, airport infrastructure, airline databases, and communication networks. Existing literature commonly presents aviation as a highly interconnected "system of systems," in which vulnerabilities in one component may affect safety, operations, and public trust across the wider ecosystem.

A major body of literature emphasizes that aviation cybersecurity is no longer limited to traditional IT protection. Ukwandu et al. (2022) conduct a systematic review of aviation cybersecurity literature and find a consistent trend toward treating cyber risks as safety-critical concerns rather than purely informational ones. This contrasts with earlier regulatory frameworks that maintained a stricter separation between safety and security domains. Similarly, Manesh and Kaabouch (2017) argue that the aviation sector's heavy reliance on networked communication systems creates an attack surface that is qualitatively different from those found in other industries, due to the real-time, safety-critical nature of aviation operations.

Taken together, the literature establishes a clear case for treating aviation cybersecurity as a multidimensional challenge involving technology, governance, and international coordination — rather than a narrow technical issue confined to IT departments.

Vulnerabilities in Communication and Navigation Systems

A significant portion of the literature focuses on vulnerabilities in aviation communication and navigation systems, particularly ADS-B (Automatic Dependent Surveillance–Broadcast) and GPS/GNSS-based technologies. Manesh and Kaabouch (2017) identify ADS-B as one of the most exposed aviation systems because its broadcast messages lack robust encryption or authentication. Unlike radar-based surveillance, ADS-B relies on aircraft self-reporting their position, making it inherently susceptible to spoofing, message injection, and false aircraft information. The authors categorize ADS-B vulnerabilities into several attack vectors — including ghost injection, flooding, and replay attacks — and note that the aviation industry's slow adoption of authentication countermeasures compounds the risk.

Khan et al. (2021) examine GPS spoofing in detail and distinguish it from the related but distinct threat of signal jamming. While jamming disrupts signal availability, spoofing is more insidious: it transmits counterfeit signals that navigation systems accept as legitimate, potentially misleading crews about aircraft position without triggering obvious alerts. The authors survey a range of spoofing detection techniques, including receiver autonomous integrity monitoring (RAIM), multi-constellation GNSS cross-checking, and cryptographic signal authentication, and find that no single method is universally effective under all operational conditions.

The AIAA (2025) publication on unreliable GPS and GNSS disruptions further documents the increasing frequency and geographic scope of signal interference incidents in aviation, particularly in conflict-adjacent regions. Together, these studies establish communication and navigation technologies as the most critical cybersecurity weak points in modern aviation, and reinforce the need for resilient alternatives and stronger authentication standards.

Airport, Airline, and Infrastructure Cyber Risks

Beyond aircraft systems, the literature highlights major cyber risks affecting airport and airline digital infrastructure. Airports and airlines increasingly rely on interconnected digital platforms for reservations,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

baggage handling, passenger information, operational control, and communication — creating a broad target surface for adversaries.

Case-based analyses in the literature illuminate the real-world impact of these risks. The British Airways data breach of 2018, for example, exposed the personal and financial data of approximately 500,000 customers and resulted in regulatory fines under the General Data Protection Regulation (GDPR), illustrating that cybersecurity failures in aviation carry both financial and reputational consequences. The ransomware-related disruption at Bristol Airport in the same year demonstrated that operational systems — including flight information displays — can be rendered inaccessible, forcing staff to revert to manual processes. These incidents contrast in character: the British Airways breach involved a sophisticated supply chain compromise, while the Bristol Airport attack exploited more conventional ransomware delivery mechanisms. The comparison highlights that aviation infrastructure is vulnerable to a wide spectrum of adversary capabilities and motivations.

The literature therefore makes clear that aviation cybersecurity must address both safety-critical aircraft systems and the broader commercial and operational technologies on which the industry depends.

Regulatory Standards and Institutional Responses

A key theme in the literature concerns the regulatory and policy frameworks developed to strengthen aviation cybersecurity. Guidance from organizations such as the International Civil Aviation Organization (ICAO), the International Air Transport Association (IATA), and RTCA/EUROCAE reflects the growing institutional recognition of cyber risk in aviation.

ICAO's Aviation Cybersecurity Strategy (2022) emphasizes cybersecurity information sharing, international cooperation, and the integration of cyber risk into the broader aviation security framework. IATA's Cyber Security Guidance Material (2021) takes a more operational focus, providing airlines and airports with practical implementation guidance on threat identification, workforce training, and incident response. While both frameworks share a commitment to collaborative risk management, they differ in scope: ICAO's mandate is primarily regulatory and intergovernmental, whereas IATA's guidance is industry-facing and voluntary.

At the technical standard level, DO-326A/ED-202A defines an airworthiness security process applicable throughout the aircraft lifecycle, from design through operational deployment. This contrasts with earlier certification standards that addressed airworthiness without explicit cybersecurity provisions. The literature suggests that while these frameworks mark meaningful progress, gaps remain — particularly regarding enforcement mechanisms and the harmonization of standards across jurisdictions.

Detection and Mitigation Approaches in Existing Literature

The literature discusses a range of techniques for detecting and mitigating cyber threats in aviation systems. Commonly proposed approaches include intrusion detection systems (IDS), anomaly detection, signal authentication, encryption, continuous monitoring, and machine learning-based classification.

Researchers note important distinctions among these methods. Signature-based IDS systems are effective against known attack patterns but struggle with novel or zero-day threats, whereas anomaly-based detection can identify previously unseen attacks but may generate higher rates of false positives in the complex, high-variability environment of aviation networks. Machine learning approaches offer the potential to improve classification accuracy over time, but Ukwandu et al. (2022) caution that their performance in civil aviation contexts remains largely unvalidated at operational scale, with most published evaluations conducted on simulated or laboratory datasets.

Signal authentication is particularly emphasized in relation to ADS-B and GPS spoofing threats. The literature generally agrees that cryptographic authentication of navigation signals would represent a significant security improvement, but implementation challenges — including the cost of retrofitting existing avionics and the need for international coordination on key management infrastructure — have delayed widespread adoption. This gap between technically feasible solutions and operational deployment represents one of the most consistent findings across the reviewed literature.

Research Gap and Relevance to the Present Study

The reviewed literature confirms that modern aviation faces cybersecurity risks across aircraft systems, airport infrastructure, communication networks, and regulatory processes. However, much of the existing work is fragmented in scope. Studies such as Manesh and Kaabouch (2017) and Khan et al. (2021) provide deep technical analyses of specific vulnerabilities but do not address the broader governance and operational context. Conversely, regulatory and policy-focused literature often does not engage in sufficient technical depth with the threat landscape it seeks to address.

This study addresses that gap by providing a structured narrative review that integrates threat categories, infrastructure vulnerabilities, response strategies, and regulatory considerations within a single unified discussion. By combining academic studies, industry reports, policy documents, and incident-based examples, the paper aims to offer a clearer overall understanding of the cybersecurity challenges facing modern aviation systems.

PROBLEM STATEMENT

In recent decades, the aviation industry has undergone profound digital transformation. Contemporary aircraft and their supporting infrastructure depend extensively on satellite communication systems, digital flight control, satellite-based navigation, networked airport management platforms, and in-flight internet connectivity. While these innovations have greatly improved operational efficiency and passenger experience, they have simultaneously introduced cybersecurity vulnerabilities that did not exist in conventional analog systems.

The increasing integration and networking of aviation systems creates growing opportunities for cyberattacks. Adversaries — including criminal organizations, hacktivists, and state-sponsored actors — can target vulnerabilities in aviation communication systems, navigation infrastructure, airline databases, and airport information platforms. Documented attack types range from passenger data breaches to GPS navigation spoofing, ransomware infections, and denial-of-service attacks against operational systems.

The persistence of legacy infrastructure further compounds this problem. Much aviation equipment was engineered before cybersecurity was embedded into design requirements, making retrofitting expensive and operationally complex. The sector also operates within a highly internationalized supply chain involving aircraft manufacturers, software vendors, airlines, airport authorities, and numerous third-party service providers, each representing a potential point of entry for adversaries.

Despite growing awareness, the aviation industry continues to struggle with adopting a holistic cybersecurity posture that adequately addresses both safety-critical aircraft systems and ground-based IT infrastructure. There is therefore an urgent need to examine the cybersecurity threats facing modern aviation comprehensively and to identify practical strategies for improving security across the entire ecosystem.

OBJECTIVES OF THE STUDY

This study is guided by the following objectives:

- To examine the expanding cybersecurity threat landscape facing modern civil aviation, including how increasing digital integration has broadened the attack surface across aircraft systems, airport infrastructure, and airline operations.
- To identify and categorize the major types of cyber threats relevant to aviation, including GPS spoofing, ADS-B manipulation, malware, ransomware, data breaches, insider threats, and denial-of-service attacks.
- To analyze the technical and organizational strategies proposed in the literature for detecting, preventing, and mitigating cybersecurity threats in aviation environments, including intrusion detection systems, encryption, anomaly detection, and zero-trust principles.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

- To examine real-world cybersecurity incidents affecting the aviation sector in order to assess the practical consequences of cyber threats and evaluate the effectiveness of existing defenses.
- To identify key gaps between proposed cybersecurity solutions and their operational deployment, and to outline directions for future research and policy development in aviation cybersecurity.

TYPES OF CYBER THREAT ATTACKS IN AVIATION

1. GPS Spoofing: GPS spoofing involves the transmission of counterfeit satellite signals designed to deceive aircraft navigation systems into computing incorrect positional data. Because modern aircraft rely heavily on GNSS for navigation, successful spoofing can compromise positional awareness and, in extreme cases, endanger flight safety. Unlike jamming, which disrupts signal availability in a detectable manner, spoofing is more insidious because the navigation system continues to function while operating on false information.

2. Signal Jamming: Signal jamming involves the broadcast of radio frequency interference to disrupt legitimate communication and navigation signals. Jamming can affect GPS/GNSS reception, VHF radio communication, and other radiofrequency systems used for air traffic control communication and navigation data exchange. While relatively unsophisticated compared to spoofing, jamming can cause significant operational disruptions, particularly in areas with limited alternative communication infrastructure.

3. Malware Attacks: Malware encompasses a broad category of malicious software — including viruses, trojans, and spyware — introduced into aviation systems such as airline databases, airport management platforms, and ground networks. Malware may be used to steal sensitive data, tamper with operational records, or disrupt system functionality. The interconnected nature of modern aviation networks means that a malware infection in one node can potentially propagate to other systems.

4. Ransomware Attacks: Ransomware is a form of malware in which attackers encrypt critical systems or data and demand payment in exchange for restoration of access. Airlines and airports are attractive ransomware targets due to their operational time-sensitivity and the large volumes of sensitive data they hold. A successful ransomware attack can cause flight delays, cancellations, and significant financial and reputational damage, as illustrated by the 2018 Bristol Airport incident.

5. Data Breaches: Data breaches occur when unauthorized actors gain access to protected systems and exfiltrate sensitive information such as passenger names, passport numbers, payment details, and travel histories. The consequences of a data breach extend beyond immediate financial loss to include regulatory penalties, reputational damage, and long-term erosion of passenger trust. The 2018 British Airways breach, which affected approximately 500,000 customers, exemplifies the scale of impact such incidents can have.

6. Insider Threats: Insider threats arise when individuals with authorized system access — whether employees, contractors, or service providers — misuse that access either deliberately (e.g., data theft or sabotage) or inadvertently (e.g., misconfiguration or mishandling of sensitive information). Insider threats are particularly challenging to detect and mitigate because they originate from within the organization's trusted perimeter.

7. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: In DoS and DDoS attacks, adversaries flood aviation systems or networks with excessive traffic, rendering them inaccessible to legitimate users. Potential targets include airline reservation portals, airport operational databases, and communication systems. While DDoS attacks do not typically compromise data integrity directly, their ability to disrupt time-critical aviation operations makes them a significant threat to service continuity.

8. ADS-B Spoofing and Message Injection: ADS-B spoofing attacks exploit the lack of robust authentication in the ADS-B protocol to inject false aircraft information into surveillance systems. An adversary can transmit fabricated position reports, create ghost aircraft tracks, or suppress legitimate signals — potentially misleading air traffic controllers and other aircraft. As Manesh and Kaabouch (2017) document, the open broadcast nature of ADS-B makes it uniquely vulnerable to this category of attack.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

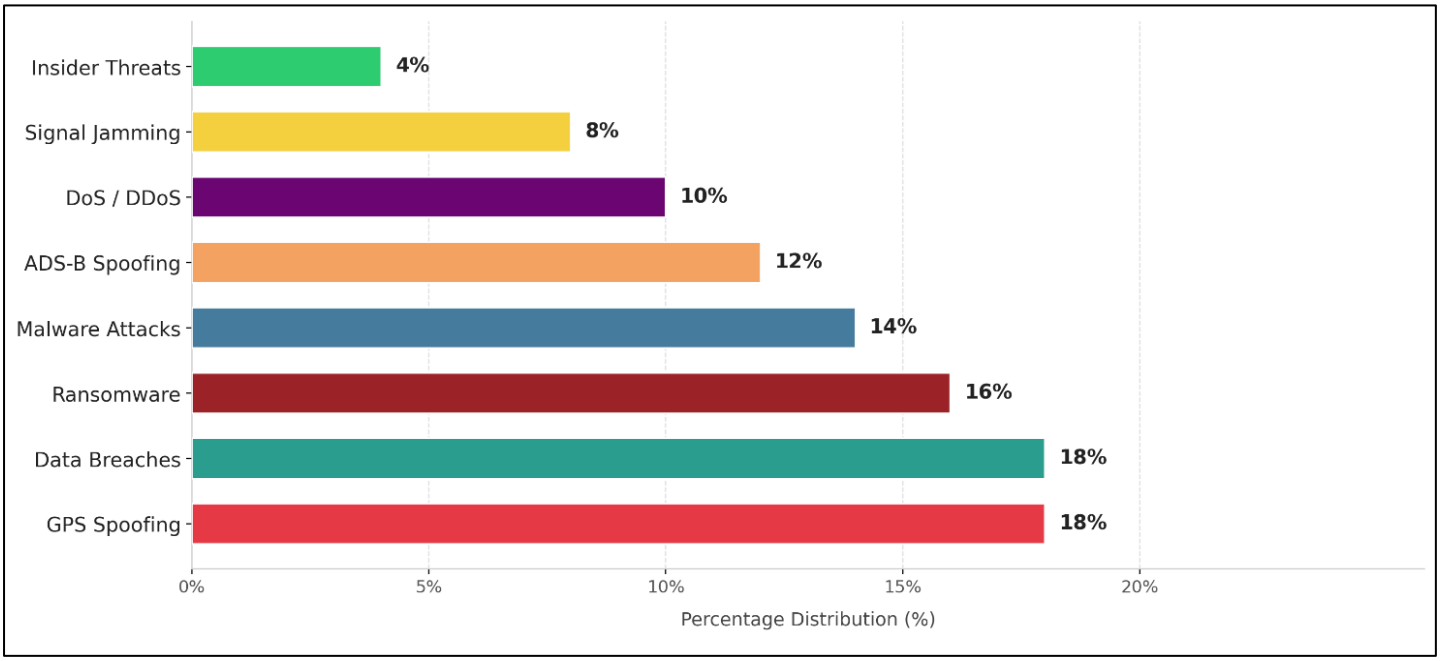

Figure 1: Types of Cyber Attacks in Aviation — Percentage Distribution

METHODOLOGY AND DATA COLLECTION

Research Design

This study adopts a qualitative narrative review design to examine cybersecurity challenges in modern civil aviation. Narrative reviews are appropriate when the objective is to synthesize and interpret a broad, multidisciplinary body of literature rather than to conduct primary experimentation or meta-analysis. Aviation cybersecurity spans aircraft systems, airport infrastructure, communication networks, regulatory frameworks, and organizational practices — a scope that makes narrative synthesis particularly suitable for providing an integrated perspective.

The study does not present original experimental data, simulations, or primary field research. Its contribution lies in the systematic organization and critical comparison of existing knowledge to identify key threats, vulnerabilities, response strategies, and gaps in current understanding.

Source Selection and Search Strategy

Relevant literature was identified through academic databases, official aviation and regulatory publications, industry reports, and documented cybersecurity incident accounts. The search focused on sources addressing civil aviation cybersecurity, digital aviation infrastructure, and cyber risk management. The following keyword combinations were used:

- “aviation cybersecurity”
- “cyber threats in aviation”
- “ADS-B vulnerabilities” or “ADS-B spoofing”
- “GPS spoofing in aviation” or “GNSS interference aviation”
- “airport cybersecurity”
- “aviation cyber risk management”
- “aviation cybersecurity regulations” or “ICAO cybersecurity”
- “intrusion detection in aviation systems”

Sources were drawn from four primary categories: peer-reviewed journal articles and conference papers; regulatory and policy documents from recognized aviation authorities; cybersecurity guidance publications from industry organizations; and credible incident reports and technology publications used for illustrative purposes.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Inclusion and Exclusion Criteria

To maintain relevance and analytical consistency, the following criteria were applied during source selection:

Inclusion criteria:

- Sources addressing cybersecurity issues specifically within civil aviation contexts
- Studies discussing aircraft systems, airport infrastructure, airline information systems, navigation or communication technologies, or aviation governance
- Peer-reviewed academic publications, official regulatory guidance, recognized industry reports, and credible incident accounts
- Sources contributing to understanding of aviation cyber threats, vulnerabilities, or mitigation strategies

Exclusion criteria:

- Sources dealing exclusively with military aviation or restricted defense systems
- General cybersecurity studies with no identifiable civil aviation relevance
- Duplicate sources or sources with weak topical relevance
- Sources lacking sufficient credibility, methodological transparency, or identifiable authorship

Data Collection

Data was collected from multiple categories of secondary sources to ensure a broad and balanced representation of the topic. Academic research papers provided the primary basis for understanding technical vulnerabilities, threat mechanics, and proposed detection and mitigation methods. Policy and regulatory documents were reviewed to analyze international governance frameworks and cybersecurity standards. Industry reports and incident case studies were used to ground the review in practical, real-world experience. Selected technology publications were consulted for information on emerging security technologies and recent threat developments.

Data Analysis

The collected material was analyzed using a thematic synthesis approach. After reviewing all selected sources, information was grouped into recurring themes that appeared consistently across the literature. These themes included: vulnerabilities in communication and navigation systems; cyber risks affecting airports and airline digital infrastructure; legacy system exposure; common threat categories such as spoofing, malware, ransomware, and data breaches; technical and organizational mitigation approaches; and regulatory and international coordination challenges. Within each theme, sources were compared and contrasted to identify areas of consensus, divergence, and evidential gaps, rather than simply catalogued.

Scope of the Study

This study focuses on civil aviation systems, including aircraft communication and navigation systems, airline digital infrastructure, airport information systems, and related cybersecurity governance frameworks. Military aviation systems are excluded, as they involve restricted information and fall outside the intended scope of this review.

Limitations

This study has several limitations. First, it relies entirely on secondary data and does not include primary experimentation, simulations, or expert interviews. Second, aviation cybersecurity is a sensitive domain in which many real incidents and vulnerabilities may not be publicly disclosed in full detail, potentially leaving significant threat vectors underrepresented in the available literature. Third, the review synthesizes sources of varying type, purpose, and methodological rigor — including academic papers, regulatory documents, and industry reports — which may introduce inconsistencies in the depth or independence of evidence. The findings should therefore be understood as a structured synthesis of publicly available literature rather than as

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

an exhaustive or experimentally validated assessment.

Ethical Considerations

The study uses only publicly available and credible secondary sources. No confidential aviation security data or restricted operational information was accessed. Proper citation and reference practices were applied throughout to maintain academic integrity and transparency.

Table 1: Data Sources Used in the Research

Source Type	Example Source	Purpose in Research
Academic Research Papers	Ukwandu et al. (2022); Manesh & Kaabouch (2017); Khan et al. (2021)	To understand aviation cybersecurity threats, system vulnerabilities, and detection techniques.
Industry Reports	IATA Cyber Security Guidance Material (2021)	To identify current cybersecurity practices, threat trends, and security recommendations.
Regulatory & Policy Documents	ICAO Aviation Cybersecurity Strategy (2022); DO-326A/ED-202A	To analyze international aviation cybersecurity standards and regulatory policies.
Case Studies / Incident Reports	British Airways data breach (2018); Bristol Airport ransomware attack (2018)	To study real-world cybersecurity incidents and understand their operational impact.
Technology Publications	AIAA (2025) on GNSS disruption; credible aviation technology news platforms	To gather updated information on recent threats and emerging security technologies.

RESULTS

The following results emerge from the thematic synthesis of secondary data drawn from academic research papers, cybersecurity reports, regulatory documents, and documented aviation cyber incidents.

Expanding attack surface: The review confirms a clear and consistent finding across the literature: the digitalization of aviation systems has substantially expanded the sector's attack surface. Modern aircraft and airport facilities rely on numerous interconnected digital components for communication, navigation, air traffic control, and passenger services. While these systems enhance operational efficiency, each represents a potential point of exploitation. The greater the degree of network integration, the larger the number of vulnerabilities that adversaries can seek to exploit.

Prevalence of identified threat types: The literature consistently identifies a core set of cyber threats relevant to aviation. GPS spoofing and ADS-B manipulation are identified as particularly high-impact threats given their potential to affect flight safety directly. Ransomware and data breaches are most commonly associated with airline and airport administrative systems. Insider threats are flagged as particularly difficult to detect and mitigate. Denial-of-service attacks are noted as a persistent risk to service continuity. These threat categories are not mutually exclusive; many real-world incidents involve combinations of attack methods.

Navigation and communication systems as primary vulnerability points: Across the reviewed literature, ADS-B and GPS/GNSS systems are consistently identified as the most vulnerable components of the aviation digital ecosystem, due primarily to their open broadcast architecture and the absence of robust authentication. Manesh and Kaabouch (2017) and Khan et al. (2021) converge on this assessment, though they differ in emphasis: the former focuses on the variety of ADS-B attack vectors, while the latter stresses the deceptive nature of GPS spoofing and the limitations of current detection approaches.

Legacy infrastructure as a compounding risk factor: A consistent finding in the literature is that legacy aviation systems — designed and certified before cybersecurity was integrated into aviation engineering

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

standards — represent a significant and persistent vulnerability. Retrofitting these systems is costly and operationally complex, and the certification processes required for avionics changes are lengthy. This creates a structural lag between the evolving threat landscape and the aviation industry's ability to respond.

Technical countermeasures: promise and deployment gap: The literature identifies a range of technical countermeasures with genuine security potential, including anomaly-based intrusion detection, cryptographic signal authentication, machine learning classification, advanced encryption, and zero-trust network architectures. However, a consistent gap is observed between conceptual proposals and validated operational deployment. Most published evaluations of machine learning-based detection, for example, are conducted on simulated rather than live aviation network data, limiting confidence in their real-world effectiveness.

Need for multi-stakeholder coordination: The review confirms that effective aviation cybersecurity cannot be achieved through technical measures alone. The aviation industry's global, multi-organizational structure means that cyber threats can exploit gaps between jurisdictions, organizations, and systems. The literature broadly endorses coordinated responses involving airlines, airports, aircraft manufacturers, software vendors, cybersecurity specialists, and international regulators — though it also identifies significant challenges in achieving consistent implementation of shared standards across this diverse stakeholder landscape.

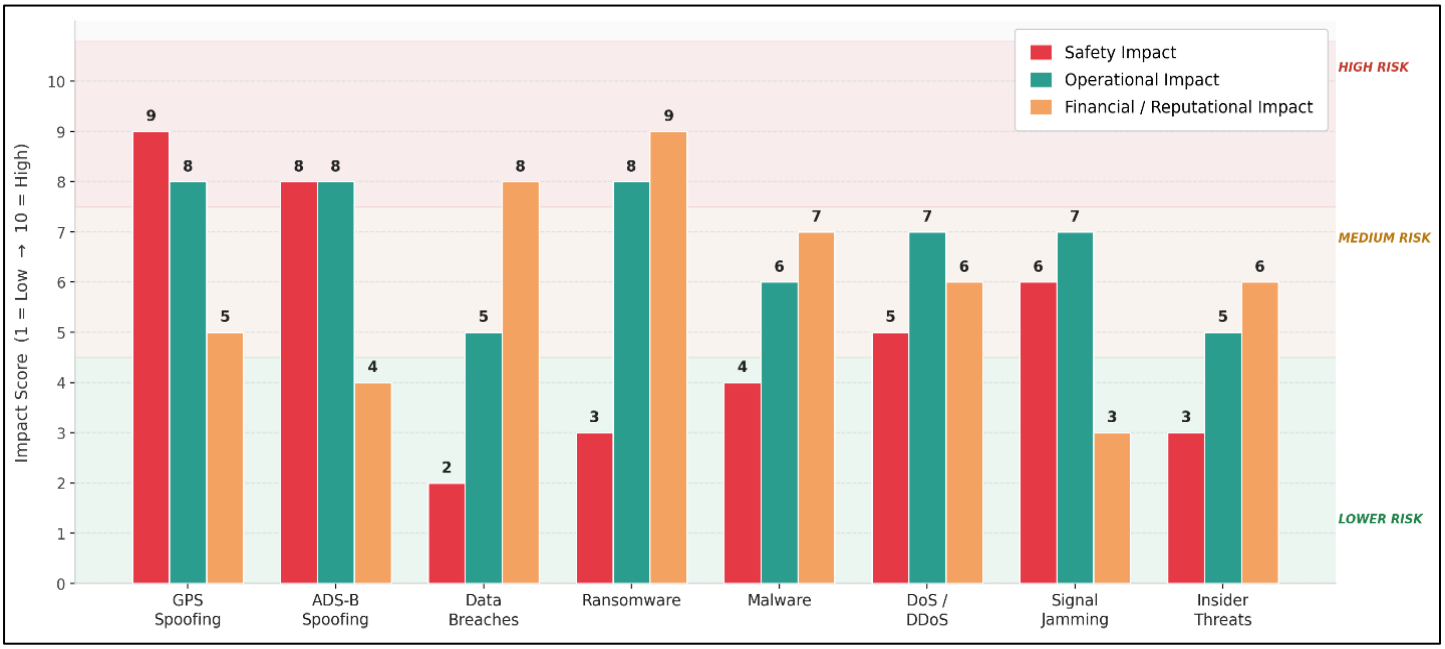

Figure 2: Key Cybersecurity Threats in Aviation Systems — Secondary Research Findings

CONCLUSION

The rapid digitalization of modern aviation has delivered transformative improvements in operational efficiency, safety management, and passenger experience. However, this digital integration has simultaneously expanded the attack surface available to adversaries, making cybersecurity one of the most consequential challenges facing the aviation sector today. As this review has demonstrated, aircraft systems, communication and navigation infrastructure, airline databases, and airport management platforms are all exposed to a diverse and evolving range of cyber threats, including GPS spoofing, ADS-B manipulation, malware, ransomware, data breaches, insider threats, and denial-of-service attacks.

The review identifies three strategic priorities that the aviation sector must address to improve its cybersecurity posture. First, navigation and communication security must be treated as an urgent technical priority. The absence of robust authentication in ADS-B and GPS/GNSS systems represents a structural vulnerability that no amount of organizational policy can fully compensate for; implementation of cryptographic signal authentication and resilient navigation alternatives should be accelerated. Second, legacy infrastructure modernization must be planned systematically. Aviation authorities and aircraft operators should develop phased roadmaps for transitioning safety-critical legacy systems to architectures that support modern

cybersecurity controls, with clear timelines and certification pathways that avoid perpetuating insecure configurations indefinitely. Third, international regulatory harmonization must be strengthened. The fragmentation of cybersecurity standards across jurisdictions — despite the global nature of aviation operations — creates exploitable seams that adversaries can leverage. ICAO's role in coordinating baseline cybersecurity requirements across member states should be expanded, and mechanisms for real-time cross-border threat intelligence sharing should be institutionalized.

More broadly, this review reinforces a finding consistent across the literature: effective aviation cybersecurity is not achievable through technical measures alone. It requires coordinated action among airlines, airports, aircraft manufacturers, software vendors, cybersecurity professionals, international regulators, and national governments. Workforce training, structured incident response procedures, and shared intelligence frameworks are as important as technical countermeasures.

Securing the digital infrastructure of modern aviation is therefore both a technical and a systemic imperative. As cyber threats continue to evolve in sophistication and scale, the aviation industry must sustain a proactive, collaborative, and multidisciplinary approach to cybersecurity — not as a compliance exercise, but as a fundamental prerequisite for the safety, efficiency, and public trustworthiness of global air transportation.

REFERENCES

1. Ukwandu, E., et al. (2022). Cybersecurity in Aviation: A Systematic Literature Review. Information, 13(3), 146. https://doi.org/10.3390/info13030146
2. Manesh, M. R., & Kaabouch, N. (2017). Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance–Broadcast (ADS-B) system. International Journal of Critical Infrastructure Protection, 19, 16–31. https://doi.org/10.1016/j.ijcip.2017.08.002
3. Khan, S., et al. (2021). GPS Spoofing Detection Techniques: A Review. IEEE Sensors Journal, 21(24), 27327–27340. https://doi.org/10.1109/JSEN.2021.3124841
4. International Civil Aviation Organization (ICAO). (2022). Aviation Cybersecurity Strategy. ICAO Publications. https://www.icao.int
5. International Air Transport Association (IATA). (2021). Cyber Security Guidance Material for Civil Aviation. IATA. https://www.iata.org
6. RTCA. (2014). DO-326A: Airworthiness Security Process Specification. RTCA Inc.
7. EUROCAE. (2014). ED-202A: Airworthiness Security Process Specification. EUROCAE.
8. AIAA. (2025). Unreliable GPS and GNSS Disruptions in Aviation: Emerging Risks and Resilient Navigation Solutions. American Institute of Aeronautics and Astronautics.