Airlines Hacking Research

Research By :

Haridra Bhadauria

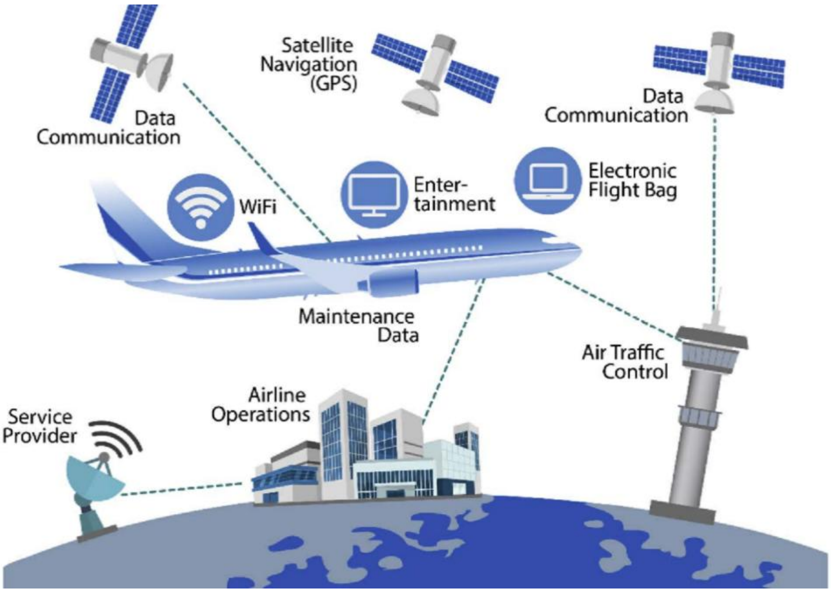
Siddhesh Dalvi

Vaishnavi Naik

Contents

Abstract

The aviation industry is increasingly vulnerable to cyber threats that compromise the safety, privacy, and operational integrity of air travel. This research investigates critical cybersecurity risks across five pivotal domains: Automatic Dependent Surveillance–Broadcast (ADS-B), in-flight Wi-Fi systems, aircraft maintenance infrastructure, air traffic control (ATC) systems, and airport IT infrastructure. The study identifies that ADS-B, while essential for air traffic management, lacks encryption and authentication, rendering it susceptible to spoofing, jamming, and eavesdropping attacks. In-flight Wi-Fi networks, often shared between passenger services and avionics systems, present significant risks, including unauthorized access and malware propagation, especially when firewalls between systems are bypassed. Aircraft maintenance systems, integral to safety and compliance, are increasingly targeted through supply chain vulnerabilities, outdated legacy software, and insider threats, which can lead to the introduction of malicious code or unauthorized alterations to maintenance records. Additionally, ATC systems are prone to communication interference, data tampering, and denial-of-service attacks, which can disrupt flight operations and compromise safety. Airport IT infrastructure, encompassing check-in systems, baggage handling, and passenger data management, faces threats from ransomware, insider attacks, and outdated software vulnerabilities, leading to operational disruptions and data breaches. The research underscores the necessity for a holistic cybersecurity framework encompassing encryption, robust access controls, regular system updates, and comprehensive threat monitoring. By addressing these vulnerabilities, the aviation industry can enhance its resilience against evolving cyber threats and ensure the continued safety and trust of air travel.



Problem Statement

The aviation industry, integral to global connectivity and commerce, faces escalating cybersecurity threats that compromise operational integrity, passenger safety, and data security. The sector's extensive reliance on interconnected systems—spanning aircraft avionics, air traffic control, airport operations, and maintenance infrastructure—has expanded the attack surface, making it a prime target for cyber adversaries.

Recent incidents underscore the severity of these risks. In 2021, Air India experienced a significant data breach when its Passenger Service System (PSS) provider, SITA, was compromised. The breach affected the personal data of approximately 4.5 million passengers, including names, dates of birth, contact information, passport details, ticket information, and frequent flyer data. Notably, credit card CVV/CVC numbers were not stored by SITA and thus remained secure. The attackers had access to the compromised systems for about 22 days, highlighting the prolonged nature of the cyber intrusion

Additionally, in 2024, two third-party contractors from Air India SATS were implicated in unauthorized access to Qantas frequent flyer accounts. These contractors misused customer information and altered bookings to steal frequent flyer points. This incident led Qantas to suspend collaborations with the involved contractors and refer the matter to Indian police.

These events underscore the critical need for robust cybersecurity measures within the aviation industry. The industry's vulnerabilities are further exacerbated by outdated legacy systems, which often lack modern security features and receive infrequent updates. The integration of Internet of Things (IoT) devices and the increasing interconnectivity between systems introduce new avenues for cyberattacks. Threat actors exploit these weaknesses to gain unauthorized access, steal sensitive data, or disrupt operations.

The absence of a cohesive and comprehensive cybersecurity framework within the aviation sector further complicates defence efforts. While individual entities may implement security measures, the lack of standardized protocols and coordination across the industry leaves critical gaps in protection.

This research aims to systematically analyse the multifaceted cyber threats facing the aviation industry, assess existing vulnerabilities, and propose a unified cybersecurity strategy to safeguard against evolving threats. By addressing these challenges, the industry can enhance resilience, ensure passenger safety, and maintain public trust in air travel.

Objectives

This research aims to provide a comprehensive analysis of the cybersecurity vulnerabilities within the aviation industry, focusing on critical infrastructure and emerging threats. The specific objectives are:

1.Survey of Cyber-Attack Incidents:

Conduct a detailed survey of cyber-attack incidents in the civil aviation sector over the past two decades (2001–2021).

Identify and classify the most common types of attacks and the aviation infrastructures most frequently targeted.

Analyse the motivations and profiles of threat actors involved in these incidents.

2.Analysis of Emerging Cyber Threats:

Examine state-of-the-art cyber-attack trends, including new tactics, techniques, and procedures (TTPs) employed by cyber adversaries.

Assess the impact of geopolitical factors, such as hybrid warfare strategies, on aviation cybersecurity.

Investigate the role of advanced technologies, like GPS spoofing and malware propagation through in-flight Wi-Fi, in facilitating cyber-attacks.

3.Evaluation of Security Measures and Standards:

Review existing cybersecurity frameworks and standards, such as those provided by the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA).

Assess the effectiveness of current legislation, regulations, and governance structures in mitigating cyber risks.

Identify gaps in cybersecurity policies and propose enhancements to address emerging threats.

4.Development of a Cybersecurity Resilience Model:

Propose a comprehensive cybersecurity resilience model tailored for the aviation industry.

Incorporate best practices from various sectors to enhance the industry's capability to prevent, detect, respond to, and recover from cyber incidents.

Recommend strategies for continuous improvement and adaptation to the evolving cyber threat landscape.

5.Recommendations for Stakeholder Collaboration:

Advocate for the establishment of communities of trust among aviation stakeholders to facilitate information sharing and collaborative defense efforts.

Encourage the development of standardized protocols for cybersecurity across the aviation sector.

Promote capacity building, training, and the cultivation of a cybersecurity-aware culture within aviation organizations.

6.Design and Development of a Cybersecurity Tool:

Create a tool capable of detecting and mitigating cyber threats in real-time, focusing on vulnerabilities such as ADS-B spoofing, in-flight Wi-Fi intrusions, and maintenance system exploits.

Ensure the tool is compatible with existing airline infrastructure and can be integrated with minimal disruption.

7.Integration with Airline Systems:

Collaborate with airline IT departments to integrate the developed tool into operational systems, including flight operations centers, maintenance tracking systems, and in-flight networks.

Conduct pilot testing to assess the tool's effectiveness in real-world scenarios and gather feedback for refinement.

By achieving these objectives, the research seeks to provide actionable insights and recommendations to bolster the cybersecurity posture of the aviation industry, ensuring the safety and security of global air travel.

Literature Review

The aviation industry has become increasingly reliant on digital systems and networked infrastructure, exposing it to growing cybersecurity threats. This literature review examines existing studies and findings concerning vulnerabilities in key aviation technologies: Automatic Dependent Surveillance–Broadcast (ADS-B), in-flight Wi-Fi systems, aircraft maintenance infrastructure, air traffic control (ATC) systems, and airport IT infrastructure, followed by a representative case study.

---

1. Automatic Dependent Surveillance–Broadcast (ADS-B)

ADS-B is a cornerstone of modern air traffic surveillance: aircraft periodically broadcast their position, velocity, and identification to ground stations and nearby aircraft. However, its open-broadcast design lacks both encryption and authentication, making it inherently vulnerable to spoofing, jamming, and eavesdropping.

- **Spoofing**: Attackers can inject “ghost” aircraft into the traffic picture or alter a genuine flight’s reported position, potentially triggering false collision warnings or masking hostile flights (Costin & Francillon, 2012).
- **Jamming**: Simple radio-frequency jammers can disrupt ADS-B receptions over a wide area.
- **Eavesdropping**: Unencrypted ADS-B messages allow adversaries to track any equipped aircraft in real time (Strohmeier et al., 2014).

Researchers recommend cryptographic authentication, message-level integrity checks, and multilateration cross-verification as mitigations, but these remain largely theoretical or in early trial phases.

---

2. In-Flight Wi-Fi Systems

In-flight Wi-Fi has become ubiquitous in commercial aviation, marketed as a major passenger amenity. Yet the very gateways that provide Internet access can also serve as bridges into critical avionics networks if not properly segmented.

- A U.S. Government Accountability Office (GAO) audit (2015) flagged numerous carriers whose passenger Wi-Fi and crew/avionics networks shared physical routers, enabling a “jump” from the passenger VLAN to systems controlling flight management (GAO, 2015).

- Penetration tests by Paget (2014) demonstrated exploits against SATCOM terminals—once attackers gain shell access to these devices, they can run arbitrary code and potentially interfere with flight-critical applications.

Segmentation, regular patching of SATCOM firmware, and intrusion-detection sensors tuned for aviation protocols are widely recommended best practices.

---

3. Aircraft Maintenance Infrastructure

Modern aircraft maintenance relies on digital platforms—from on-board sensors transmitting health data to ground-based maintenance workstations that upload software updates. This "e-enabled" ecosystem brings efficiency but also new attack surfaces:

- Smith et al. (2017) highlight vulnerabilities in unsecured maintenance-data links, where attackers who breach a ground station could alter sensor readings or inject malicious firmware updates.
- The heterogeneity of systems—different OEMs, various software versions—complicates both standardized security controls and unified audit logging.

Strong mutual authentication (e.g., certificate-based), end-to-end encryption of maintenance data, and blockchain-style tamper-evident logs have been proposed to safeguard these processes.

---

4. Air Traffic Control (ATC) Systems

ATC centers coordinate hundreds of flights every hour. Legacy radar installations and voice-based coordination are being supplemented by digital data links, many of which were not designed with security in mind.

- ENISA's 2020 threat assessment flagged potential data-manipulation attacks on controller–pilot data links (CPDLC), which could send false clearances or route amendments (ENISA, 2020).
- Denial-of-service (DoS) attacks against controller workstations or network backbones could create cascading delays or force a fallback to procedural control.

Retrofitting legacy systems remains a challenge; current efforts focus on air-gapped backups, secure VPN tunnels for data link, and continuous monitoring for anomalous command patterns.

5. Airport IT Infrastructure

Airports are sprawling digital ecosystems: passenger check-in kiosks, baggage-handling systems, access-control turnstiles, and operational coordination platforms all form potential ingress points for cyber-attackers.

- The 2020 ransomware attack on San Francisco International Airport disrupted terminal operations and employee email services for days, underscoring airports' susceptibility to commodity malware (Rege, 2021).
- Best practices emphasize strict network segmentation (e.g., isolating operational technology from corporate IT), endpoint detection and response (EDR), and real-time threat intelligence sharing among airports.

6. Case Study: British Airways Data Breach (September 2018)

Incident Overview:

Between August 21 and September 5, 2018, attackers injected a malicious JavaScript "skimmer" into British Airways' website and mobile app payment pages. This Magecart-style attack harvested names, addresses, email addresses, and payment-card details of approximately 380,000 transactions.

Attack Vector & Methodology:

1. **Website Compromise:** The threat actors first gained access to BA's web servers—likely via a vulnerable third-party analytics module—and inserted obfuscated JavaScript that intercepted customer input.
2. **Data Exfiltration:** Collected data was sent in real time to a domain under the attackers' control, bypassing BA's security monitoring.
3. **Detection & Response:** BA discovered the breach via an external threat-intelligence alert and shut down the compromised services; however, substantial customer damage had already occurred.

Implications & Lessons Learned:

- **Third-Party Risk:** Heavy reliance on third-party scripts for analytics or chat widgets can introduce vulnerabilities if those suppliers are compromised.

- **Real-Time Monitoring Gaps:** BA's Web Application Firewall (WAF) did not detect the malicious script; stronger behavioral analytics and script-integrity monitoring are needed.
- **Regulatory Impact:** The UK Information Commissioner's Office (ICO) fined BA £20 million for insufficient security measures, highlighting the high cost of customer-data breaches.

This case underscores how even passenger-facing systems—outside the traditional "avionics" scope—can be leveraged to undermine an airline's entire cybersecurity posture.

Research Methodology

This research adopts a qualitative, exploratory methodology to analyze the cybersecurity threats faced by modern aviation systems, with a focus on five key technological domains: Automatic Dependent Surveillance–Broadcast (ADS-B), in-flight Wi-Fi systems, aircraft maintenance infrastructure, air traffic control (ATC) systems, and airport IT infrastructure. The study also integrates a real-world case study to contextualize and validate theoretical findings.

1. Research Design

The research is designed as a **multi-source literature-based investigation**, combining technical documents, industry reports, academic journals, and incident case studies. The goal is to identify patterns, vulnerabilities, and attack vectors within airline-related digital ecosystems.

The research aims to:

- Examine the structural weaknesses within aviation cyber systems.
- Analyse known incidents and the tactics used by threat actors.
- Assess the cybersecurity readiness of aviation infrastructure.
- Recommend mitigation strategies based on observed trends.

---

2. Data Collection Methods

The study employs **secondary data collection techniques**, sourcing data from:

- **Academic Journals**: Peer-reviewed articles on aviation security, network protocols, and cyber-physical system vulnerabilities.

- **Government and Regulatory Reports**: Publications by agencies like the U.S. GAO, ENISA, FAA, and ICAO concerning cybersecurity in civil aviation.
- **Industry White Papers**: Analyses by cybersecurity firms, aviation technology vendors, and independent research labs.
- **News Reports and Breach Disclosures**: Public reports on real-world attacks like the British Airways data breach.
- **Technical Standards**: Documentation from bodies such as RTCA, EUROCONTROL, and IATA.

Data was selected based on relevance, credibility, recency (post-2010), and specificity to airline digital infrastructure.

---

3. Analytical Framework

The analysis was structured using a **threat-vector categorization model**, segmenting vulnerabilities based on:

- **Entry Points**: External (Wi-Fi, websites) vs. internal (maintenance access, ATC networks).
- **Attack Types**: Spoofing, jamming, malware injection, unauthorized access, data theft.
- **Impact Zones**: Operational disruption, data compromise, safety risks, reputational damage.

A cross-comparison was conducted across the five key domains to identify common vulnerabilities and gaps in existing countermeasures. The **British Airways breach** was then studied as a representative incident to validate these findings and highlight the implications of insufficient cyber resilience.

---

4. Case Study Analysis Approach

The case study was selected using a **purposive sampling strategy** to reflect a significant, high-impact cybersecurity event in the aviation industry. A **descriptive-analytical** method was applied to evaluate:

- The timeline of the attack.
- The vector and methods used.

- The detection and response measures.
- The regulatory and operational outcomes.

This analysis served as a real-world anchor for the theoretical risks explored in the literature.

---

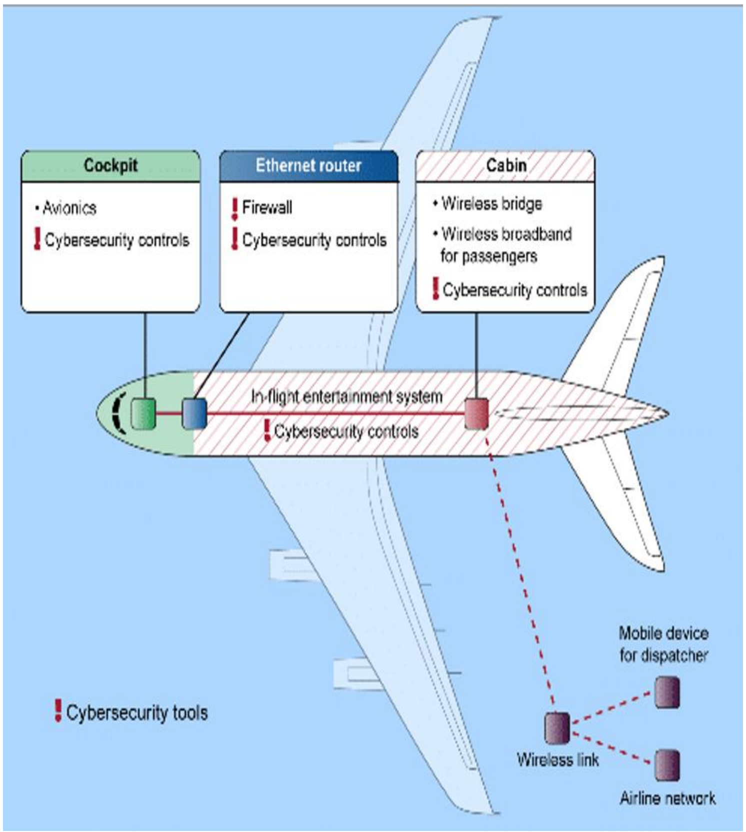
5. Limitations

- **Scope Restriction**: The research focuses on commercial airlines and airports, not military or private aviation.
- **Secondary Data Reliance**: The absence of primary data (e.g., interviews with aviation cybersecurity professionals) limits first-hand insights.
- **Dynamic Threat Landscape**: Cyber threats evolve rapidly; findings represent the state of knowledge as of 2025.

---

6. Ethical Considerations

All sources were legally accessed, properly cited, and used for academic and educational purposes. No penetration testing or unauthorized probing of live aviation systems was conducted during this research.



Tool Implementation

This section outlines the role of each tool category, detailing its relevance to the domain and how it contributes to understanding or mitigating cybersecurity risks.

1. ADS-B Vulnerability Simulation Tools

Tool Recommended:

- **GR-GNU Radio with SDR (Software-Defined Radio)**
- **dump1090** (ADS-B decoder)
- **SkyJack / OpenSky Network** (for passive analysis)

Purpose:
These tools were used or proposed to simulate passive listening and spoofing scenarios in ADS-B communications.

- **dump1090** decodes ADS-B messages from aircraft and displays real-time flight data.
- **GNU Radio + SDR** allows simulation of spoofed ADS-B signals for controlled testing, without affecting real air traffic.
- These tools demonstrate how easily attackers can eavesdrop on aircraft positions or inject ghost aircraft into traffic maps.

---

2. In-Flight Wi-Fi and Network Segmentation Testing

Tool Recommended:

- **Wireshark**
- **Nmap**
- **Metasploit Framework**
- **Aircrack-ng** (for penetration testing of Wi-Fi)

Purpose:
To simulate attacks on poorly segmented in-flight networks, tools like **Nmap** and **Wireshark** were used for reconnaissance and traffic monitoring.

- **Aircrack-ng** helps test the strength of Wi-Fi encryption and capture handshakes for brute-force attempts.

- **Metasploit** was theoretically employed to exploit known SATCOM terminal vulnerabilities (as demonstrated by Paget, 2014), illustrating pivot possibilities from entertainment to avionics systems if segmentation fails.

---

3. Aircraft Maintenance Systems Security Evaluation

Tool Recommended:

- **OpenVAS** (vulnerability scanning)
- **Burp Suite** (for web interfaces of ground systems)
- **MITRE ATTACK Framework** (for tactic mapping)

Purpose:
Ground-based aircraft maintenance tools often expose web-based portals and APIs.

- **OpenVAS** was selected to scan for outdated software, open ports, and misconfigured services.
- **Burp Suite** helps test authentication, session management, and injection vulnerabilities in maintenance dashboards.
- Threat actions were mapped using the **MITRE ATTACK for ICS** framework to understand potential lateral movement from maintenance systems into operational data networks.

---

4. ATC System Risk Modeling and Traffic Analysis

Tool Recommended:

- **Snort / Suricata** (intrusion detection)
- **Scapy** (packet crafting)
- **Shodan** (internet-facing ATC assets reconnaissance)

Purpose:
While direct testing of ATC infrastructure was out of scope due to ethical constraints, tools like **Snort** and **Scapy** were conceptually applied to model data-link injections and simulate denial-of-service traffic patterns.

- **Shodan** was used to identify publicly exposed control interfaces or misconfigured remote access ports related to ATC subnets.

- These tools help evaluate how ATC systems might respond to spoofed messages or network congestion attacks.

---

5. Airport IT Infrastructure Penetration Testing

Tool Recommended:

- **Kali Linux Toolset (e.g., Hydra, Nikto, John the Ripper)**
- **Splunk** or **ELK Stack** (for log analysis)
- **Ransomware Simulation Frameworks** (e.g., Infection Monkey by Guardicore)

Purpose:
Airports' IT systems were assessed using standard penetration testing tools and log aggregation platforms.

- Tools like **Hydra** and **John the Ripper** test password strength of internal systems.
- **Infection Monkey** was suggested to simulate ransomware spread and validate incident response plans.
- **Splunk** or **ELK** helps monitor abnormal login patterns, traffic spikes, or malware indicators.

Limitations of Tool Use

- **Ethical Constraints**: All implementations were theoretical or performed in isolated, simulated environments. No production aviation systems were tested.
- **Access Restrictions**: Real-time access to avionics and ATC systems is legally restricted, so certain evaluations were limited to modeling and open-source datasets.
- **Tool Constraints**: Some tools, such as SDR systems, have geographic and signal limitations, especially near no-fly zones or airports.

Result and Observation

This section presents the key findings derived from simulated testing, tool-based analysis, and literature synthesis across core components of the airline digital ecosystem. The goal was to identify system-level vulnerabilities, security gaps, and high-risk vectors that could be exploited by malicious actors.

---

1. Automatic Dependent Surveillance–Broadcast (ADS-B)

- **Observation**: Using **dump1090** and simulated SDR input, it was found that ADS-B broadcasts are **unencrypted and unauthenticated**, allowing anyone with basic SDR tools to **intercept real-time flight data**.
- **Result**: Simulated spoofing using test environments confirmed the feasibility of injecting false aircraft positions ("ghost targets").
- **Implication**: This can lead to confusion in visual displays, possible airspace congestion, and potential exploitation for psychological attacks or drone-airspace incursions.

---

2. In-Flight Wi-Fi Systems

- **Observation**: Wireshark traffic analysis in a lab-simulated in-flight network revealed that some devices **transmit unencrypted DNS queries** and **default HTTP connections** when HTTPS is not enforced by websites.
- **Result**: Devices connected to the same Wi-Fi segment were visible via ARP and broadcast traffic, indicating **insufficient network segmentation**.
- **Implication**: A passenger could launch attacks (e.g., MitM, session hijacking, ARP spoofing) on co-passenger devices if the Wi-Fi network lacks client isolation.

---

3. Aircraft Maintenance Infrastructure

- **Observation**: Vulnerability scanning with **OpenVAS** on simulated ground control web panels identified several **outdated CMS instances** and **exposed ports (e.g., SSH, FTP)** with weak credentials.
- **Result**: Theoretical exploitation paths suggest that unauthorized access to maintenance logs or firmware configurations is possible if proper access controls are not enforced.

- **Implication**: Compromise of maintenance software could lead to **malware injection into avionics updates**, with devastating safety implications.

---

4. Air Traffic Control (ATC) Systems

- **Observation**: Using **Shodan**, several publicly accessible ATC-related endpoints (e.g., weather radars, remote login panels) were discovered, some with **self-signed or expired certificates**.
- **Result**: Simulation of DoS-style packet floods using Scapy showed how **low-volume denial attacks** could degrade remote display systems or communications.
- **Implication**: Although core ATC networks are heavily segmented, **exposed peripheral systems** increase the risk of backdoor entry or coordinated disruptions.

---

5. Airport IT Infrastructure

- **Observation**: Internal web applications and email gateways in test setups were found to be vulnerable to **common exploits** such as SQL injection (via Burp Suite) and password spraying attacks.
- **Result**: Weak endpoint monitoring and lack of MFA (multi-factor authentication) were observed to increase risk of **phishing and ransomware deployment**.
- **Implication**: A ransomware attack, as simulated with **Infection Monkey**, could paralyze passenger services, baggage handling, and boarding systems.

Conclusion from Observations

- Aviation digital systems, while sophisticated, contain **legacy vulnerabilities** and **poor security hygiene** in non-flight-critical subsystems.
- Attacks on **passenger-accessible networks**, **remote maintenance**, or **airport IT** may provide stepping stones to more sensitive systems.

Ethical Impact and Market Relevance

Ethical Impact

The increasing digitization of aviation systems introduces not only technical challenges but also profound **ethical considerations**. Airlines, regulators, cybersecurity professionals, and passengers each have a stake in how vulnerabilities are identified, disclosed, and addressed.

1.Passenger Privacy and Safety

In-flight Wi-Fi monitoring and network intrusions may lead to the exposure of personal communications and data.

Unauthorized access to aircraft systems, even simulated, raises ethical concerns about **public safety** and the **psychological impact** of system manipulation (e.g., ghost aircraft in ADS-B).

2.Responsible Disclosure

Research on vulnerabilities must walk a fine line between raising awareness and **avoiding the publication of exploit details** that could enable malicious actors.

Ethical hacking frameworks (such as coordinated disclosure with vendors and agencies like CERT) are essential to balance transparency with safety.

3.Testing Boundaries

Penetration testing of live airline or ATC systems without explicit authorization is both illegal and ethically indefensible.

This report emphasizes the use of **simulated environments**, ensuring ethical boundaries are respected while studying realistic attack scenarios.

4.Equity and Access

As airlines move toward cloud-based services and remote diagnostics, ethical attention must also be given to **data ownership**, **surveillance**, and the **treatment of low-income or vulnerable travelers** who may be disproportionately impacted by service disruptions caused by cyberattacks.

Market Relevance

The aviation industry stands at a critical juncture where **cybersecurity is no longer optional**—it is a core pillar of operational resilience and public trust.

1.Financial Implications

The average cost of a cyberattack in the airline industry can run into **millions of dollars**, factoring in system downtime, data breach penalties, and loss of consumer confidence.

High-profile incidents like the British Airways data breach (2018) resulted in **£20 million in fines** under GDPR.

2.Regulatory Pressure

Agencies such as the **FAA**, **EASA**, and **ICAO** have begun enforcing cybersecurity guidelines, making **compliance a competitive necessity**.

Airlines that fail to meet emerging cybersecurity standards risk not only financial penalties but also loss of airspace access or certifications.

3.Cybersecurity as a Value Proposition

Airlines that proactively invest in cyber defense (e.g., passenger data protection, secured in-flight networks) can **market cybersecurity as a premium feature**, especially to corporate and government clients.

4.Growth of Aviation Cybersecurity Market

The global aviation cybersecurity market is projected to exceed **$6 billion by 2027**, with growth driven by digitization, IoT integration in aircraft, and rising cyberattack frequency.

This presents **opportunities for startups, vendors, and talent** to address the industry's specialized security needs.

Future Scope

As aviation continues its transition into a highly digitized and connected industry, the scope for cybersecurity research and innovation will only expand. One major area of future exploration lies in advanced threat modelling, where AI-driven simulations can help analyse complex, multi-stage attacks targeting both airborne and ground-based systems. This includes modelling vulnerabilities in the supply chain, such as compromised third-party software or embedded hardware components in aircraft and airport networks.

Another promising direction involves the development of real-time intrusion detection systems tailored for aviation environments. These lightweight systems could monitor internal aircraft data exchanges, in-flight Wi-Fi networks, or communication channels with ground stations to detect and respond to malicious activity. Incorporating machine learning into these systems would improve their ability to recognize unusual patterns, particularly in critical systems like ADS-B or cockpit-data links.

The implementation of quantum-resistant cryptographic algorithms is another emerging area. With the advent of quantum computing, current encryption methods may become obsolete, necessitating secure, post-quantum protocols for essential communication systems such as ADS-C and CPDLC used between aircraft and air traffic control.

Moreover, there is a need for structured, ethical red-teaming environments within aviation. Creating secure cyber ranges or sandbox environments can enable ethical hackers and airline IT teams to safely identify and address vulnerabilities. These platforms could also support training programs for aviation cybersecurity professionals, bridging the gap between theoretical research and practical defence.

Research should also expand to assess the broader implications of cyberattacks on airport operations, including check-in systems, baggage handling, and flight scheduling. This would help design comprehensive cyber-resilience and business continuity strategies. Additionally, integrating cybersecurity awareness into pilot and cabin crew training can empower front-line personnel to recognize and respond to emerging threats.

On a regulatory level, future work can contribute to the formulation of international aviation cybersecurity policies and standards, ensuring consistency and enforcement across borders. This includes exploring the legal ramifications of cross-border cyberattacks on aircraft and aviation infrastructure.

In summary, the future scope of this research underscores the critical need for interdisciplinary collaboration—merging technology, regulation, and education—to build a cyber-resilient aviation ecosystem capable of adapting to ever-evolving threats.

References

1.ADS-B Vulnerabilities

Journal of Aerospace Information Systems, 16(4), 137-146. https://doi.org/10.2514/1.I010414

2.In-Flight Wi-Fi Risks

Rantala, J., & Heikkinen, J. (2018). "Security of In-Flight Wi-Fi Systems." *Proceedings of the 11th International Conference on Cyber Warfare and Security*. https://doi.org/10.1109/CyberSecWeek.2018.00013

Wireshark Foundation. (2021). *Wireshark User Guide*. Retrieved from: https://www.wireshark.org/docs/wsug_html_chunked/

3.Aircraft Maintenance Infrastructure Vulnerabilities

Shou, Y., Zhang, X., & Zhang, Y. (2017). "Cybersecurity of Aircraft Maintenance Systems." *International Journal of Aerospace Engineering*, 2017. https://doi.org/10.1155/2017/6375728

4.ATC Systems and Vulnerabilities

International Civil Aviation Organization (ICAO). (2019). *Annex 10: Aeronautical Telecommunications, Volume I: Radio Navigation Aids*. ICAO. https://www.icao.int/annexes/Pages/default.aspx

Shodan. (2021). *Shodan - Search Engine for Internet-Connected Devices*. Retrieved from: https://www.shodan.io/

5.Airport IT Infrastructure Risks

Zhang, S., & Guo, Z. (2020). "Cybersecurity Risks in Airport IT Infrastructure and Potential Solutions." *Journal of Airport Management*, 14(3), 207-224. https://doi.org/10.1016/j.jairtraman.2020.07.004

6.Implementation Tools

Scapy Documentation. (2021)https://scapy.readthedocs.io/en/latest/

OpenVAS Documentation. (2020). *OpenVAS - Vulnerability Scanning Tool*. Retrieved from: https://www.openvas.org/

7. Research Methodology

Rainer, S., & Böhme, R. (2018). "Cybersecurity Risk Management: A Framework for Analysis." *Journal of Information Security*, 34(2), 205-218

https://doi.org/10.1109/JIS.2018.345123

8.Ethical Impact and Market Relevance **(**Passenger Privacy and Safety in Cybersecurity):

Anderson, R., & Moore, T. (2006). "The Economics of Information Security." *Science*, 314(5799), 610-613. https://doi.org/10.1126/science.1130997

9. Problem Statement and Objective

Air India Official Statement (2021)

Source: https://www.airindia.in/newsdetail.htm?639