


CYBERSECURITY in the TRANSPORTATION INDUSTRY

Edited By
Imdad Ali Shah
Noor Zaman Jhanjhi

Scrivener Publishing
WILEY

Cybersecurity in the Transportation Industry

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Cybersecurity in the Transportation Industry

Edited by
Imdad Ali Shah
and
Noor Zaman Jhanjhi

WILEY

This edition first published 2024 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

ISBN 9781394204267

Front cover images supplied by Pixabay.com and Adobe FireFly
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Acknowledgments

We would like to express our thanks to Almighty Allah SWT for his all blessings and then great appreciation to all of those we have had the pleasure to work with during this project. The completion of this project could not have been accomplished without their support. First, the editors would like to express deep and sincere gratitude to all the authors who shared their ideas, expertise, and experience by submitting chapters to this book and adhering to its timeline. Second, the editors wish to acknowledge the extraordinary contributions of the reviewers for their valuable and constructive suggestions and recommendations to improve the quality, coherence, and content presentation of chapters. Most of the authors also served as referees. Their willingness to give time so generously is highly appreciated. Finally, our heartfelt gratitude goes to our family members and friends for their love, prayers, caring, and sacrifices in completing this project well in time.

Imdad Ali Shah,
Scholar
School of Computing Science, Taylor's University, Malaysia
Prof. Dr. Noor Zaman Jhanjhi,
Taylor's University, Subang Jaya, Selangor Malaysia
Program Director for Postgraduate Research Programs

1

Cybersecurity Issues and Challenges in Civil Aviation Security

Imdad Ali Shah[1]*, N.Z. Jhanjhi[1] and Sarfraz Brohi[2]

[1]School of Computing Science, Taylor's University, Kuala Lumpur, Selangor, Malaysia
[2]University of the West of England (UWE), Bristol, United Kingdom

Abstract

It is crucial to remember that security protocols for civil aviation are constantly updated and assessed to reflect new threats and technological advancements. Even though these precautions greatly increase security, there is always a chance of hijacking. However, the objective is to reduce the risk of such situations occurring and to assure immediate response and resolution in the event that they do. Aviation security is an essential aspect of modern-day air travel. It involves a range of measures designed to protect passengers, crew, and aircraft from unlawful interference such as hijacking, terrorism, and sabotage. The software components of these systems are increasingly at risk due to their interconnectedness. These concerns are expected to increase as the aviation industry rolls out increasingly electronic-enabled planes and smart airports. Trends and lessons from a 20-year analysis of aviation cybersecurity risks and attack surfaces might guide future frameworks to defend a vital industry. Cybercriminals, especially nation-state actors and terrorists, are increasingly drawn to the aviation industry as it grows more digitised and dependent on wireless technology. Malicious actors can take advantage of vulnerabilities in designing and implementing the vast number of linked devices and subsystems. The aim of this chapter is to provide an overview of the aviation infrastructure's weak spots in terms of the threat actors and attack methods that are most likely to be used during persistent attack operations. The sector will benefit from the analyses by better understanding its current and future cybersecurity measures. According to information currently available, state actors and persistent advanced threat groups working together to enhance local aviation capacities and track, permeate, and compromise the abilities of other sovereign

**Corresponding author*: shahsyedimdadali@gmail.com

Imdad Ali Shah and Noor Zaman Jhanjhi (eds.) Cybersecurity in the Transportation Industry, (1–24) © 2024 Scrivener Publishing LLC

countries pose the greatest risks to the aerospace industry. Malicious hacking is the most common attack on the aviation industry's computer infrastructure. Air Traffic Management (ATM) uses Safety Management Systems (SMS) to implement safety policies, practices, and procedures in compliance with international standards. SMS effectiveness is crucial to ATM safety in a changing operating environment. The primary objective of this chapter is to peer-review civil aviation security issues and challenges. Our recommendations and ideas will help the civil aviation industry and new researchers.

***Keywords*:** Cybersecurity risk, aviation, security issues and challenges and management systems

1.1 Introduction

Protecting airports, airspace, aircraft, passengers, crew, and the public, checked and carry-on luggage, freight, mail, and food service supplies from criminal activities like hijacking, sabotage, and terrorism is what aviation security is all about.

Concerns about the durability of existing cybersecurity protection frameworks have arisen considering the continued trend toward greater Information and Communications Technology (ICT) tools and mechanical instruments that are often employed in the field of aviation. With the introduction of "smart airports" and "e-enabled aircraft infrastructures," the aviation industry faces new challenges, one of which is meeting the sector's requirements for cybersecurity compliance [1–3]. When it comes to connecting different countries, the aviation industry is in a prime position. Since even seemingly minor mistakes can have catastrophic results, such as the loss of life or the exposure of sensitive information belonging to stakeholders, employees, and customers, or the theft of credentials, intellectual property, or intelligence, it is crucial that the infrastructures supporting its operational integrity be robust [4–6]. Significant threat actors are working with state actors to steal aerospace secrets and improve their own domestic aerospace capabilities while also monitoring, infiltrating, and subverting the capabilities of other countries. The operational security of a vital sector of the economy must be safeguarded from cybercriminals, making it an urgent priority to develop and deploy effective cyber defences. Figure 1.1 presents the cyberattack types.

The fact that there are so many airports in the United States (5,080 public and 14,556 private as of 2019) may have something to do with the high

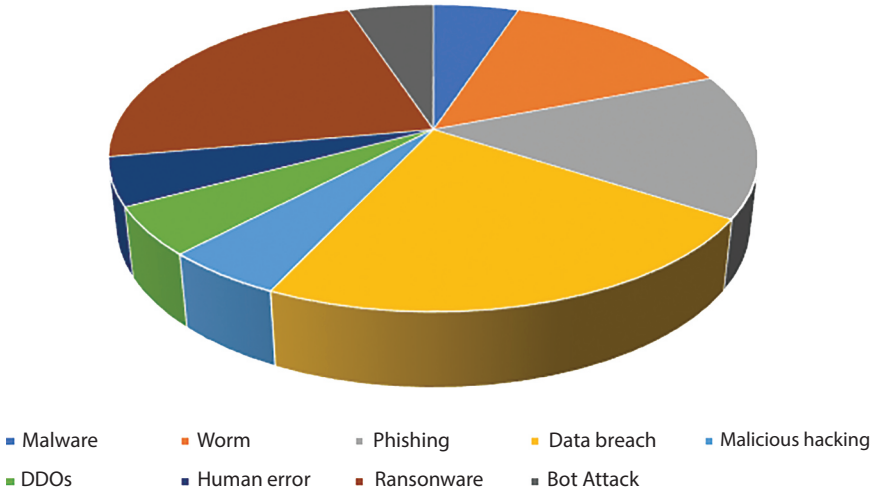

Figure 1.1 Cyberattacks by type.

number of occurrences. Britain tops the list of countries attacked by a wide margin, with the rest of Europe coming in second at a rate of 44%. Airports in Africa have never been the target of a cyberattack, and Asia ranks third with 8%. The frequency with which airports were closed and the length of time aeroplanes were grounded because of cyber incidents varies [7–9]. We compile information from the literature on the various types of cyberattacks, the actors behind them, and their motivations. Figure 1.2 presents the cyberattacks in aviation.

The third section analyses the recorded cyberattacks over the past two decades, while the fourth identifies potential entry points for cybercriminals in airports and aviation systems. Cybersecurity threats in the civil

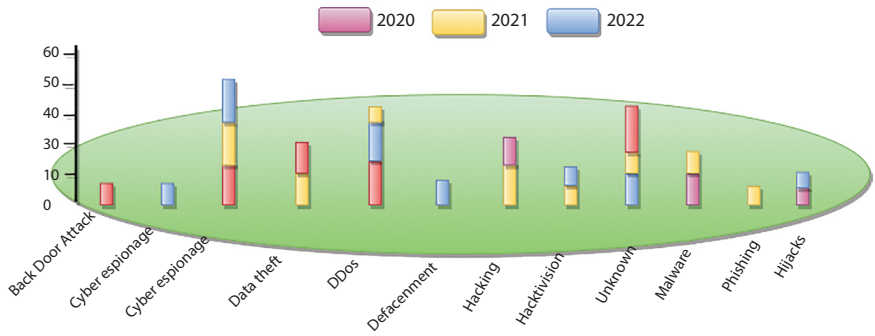

Figure 1.2 Cyberattacks on aviation.

aviation sector are discussed. Although traditional risks may appear differently during and after the Covid-19 pandemic, incident management, teamwork, and security assurance remain critically important throughout [10–12]. Furthermore, the sector must consistently adapt to the evolving regulations and challenges imposed by the global security environment to expand and evolve its operations. While bolstered security is always an advantage, it can also boost operational efficiencies inside a company, strengthen relationships between airports, airlines, and aviation authorities, and increase consumer happiness.

The chapter focuses on the following points:

- Peer-reviews cybersecurity measures in civil aviation
- Technologies in the civil aviation sector
- Security issues and challenges in the civil aviation sector
- Cyberattacks and hijacking incidents in the aviation industry
- Cyber issues and challenges.

1.2 Literature Review

There are several threats to civil aviation that must be addressed with consistent resources. To overcome these obstacles and guarantee the safety of air travel for passengers and crew, a cooperative strategy including governments, airlines, airports, and security agencies is essential. Cybersecurity is a major concern in the aviation industry because of the widespread adoption of digital technologies. Aircraft and their data are vulnerable to cyber risks such as hacking, malware, and phishing [13–15]. The aviation industry, including airports and airlines, is susceptible to insider threats from anyone having access to restricted areas, such as employees. Airline security relies heavily on the screening of passengers. Procedures for screening passengers and their belongings must be thorough enough to identify forbidden objects, including firearms, explosives, and other harmful materials. Passenger screening has certain benefits, but it also has drawbacks, such as lengthy lines, delays, and privacy issues [16–19]. Aviation security must continually adapt to new and emerging threats [20], including drones, which could be used for terrorist attacks or other malicious purposes, and new types of explosives or weapons that are difficult to detect. Civil aviation security is a global issue that requires international coordination and cooperation. The lack of consistency in security measures across different countries and regions can create vulnerabilities and increase the risk of incidents. Figure 1.3 presents the cyberattack types.

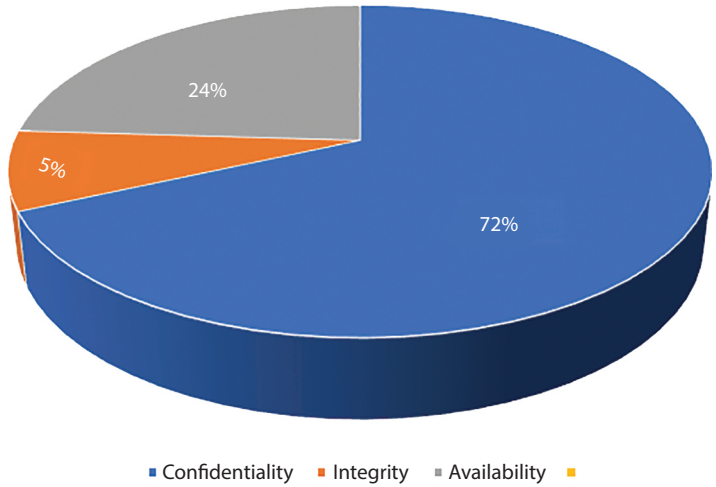

Figure 1.3 Cyberattack types.

North America is home to the most cyberattacks in the aviation industry, with 11 of the 26 occurrences occurring in the United States of America (USA) and only one in Canada. There were 5,080 public and 14,556 private airports in the United States in 2019, according to [21–23]. Therefore, the high number of occurrences may be related to this high concentration of airports. Britain tops the list of countries attacked by a wide margin, with the rest of Europe coming in second at a rate of 44%. Airports in Africa have never been the target of a cyberattack, and Asia ranks third with 8%. The frequency with which airports closed and the length of time airplanes were grounded because of cyber incidents varies. Figure 1.4 shows the Taxonomy of Civil Aviation Security.

The likelihood of cyber mishaps has increased due to the growing dependence on data integrity and privacy for the efficient operation of daily commercial operations. A significant pillar of the development of [24–26] next-generation systems, increased automation opens more entry points for malicious actors. According to Cyber Risk International [27–30], the proliferation of cybersecurity threats is due to a confluence of factors, including digital transformation, increased interconnectedness, segmentation, and complexity, and new industry solutions to accommodate the rising demand for international travel. The most important takeaways are as follows: Increased risk of cyberattacks is a direct result of the industry's increasing reliance on IT infrastructure to keep up service quality, as well as other factors such as the proliferation of new players and the persistence

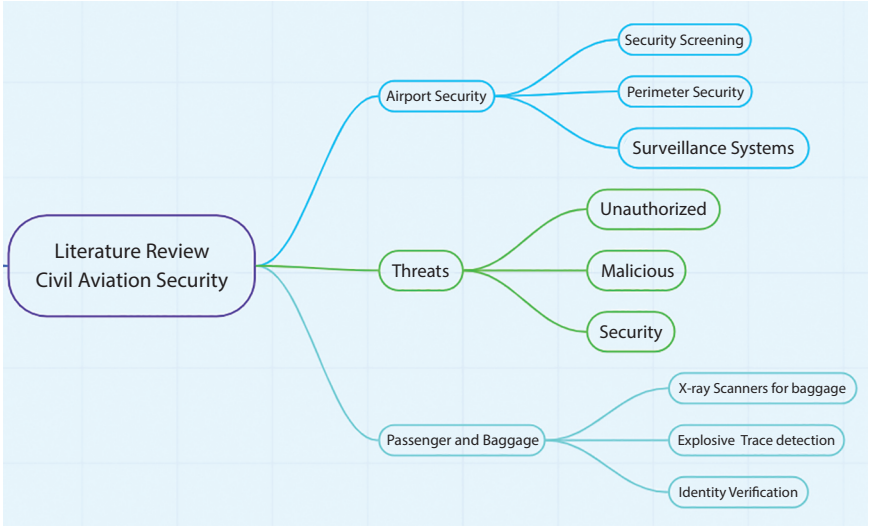

Figure 1.4 The taxonomy of civil aviation security.

of long-standing problems in the IT infrastructure that were never intended to deal with the threats posed by cybercriminals [31–33]. In addition to a lack of money, manpower, and current operational technologies like Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), insider threats and the inability to upgrade legacy systems are also cited as problems. Solutions include creating a culture of security and executing effective measures of prevention and proactivity. There are growing threats and difficulties in ensuring adequate cybersecurity due to the rising reliance on data-driven operations to boost company efficiency and citizen well-being. Integration of technologies has unquestionably improved the security and efficacy of air travel. Nevertheless, increased human mobility and hyperconnectivity open the floodgates to a cascading impact, where a cyber incident at one airport becomes a worldwide problem with social and economic ramifications [34–36]. Industry must consequently take the initiative to supply effective defences against any new type of attack.

1.3 Research Methods

There are four platforms used for the collected data for this chapter; the procedure flowchart for gathering data is shown in Figure 1.5. We used

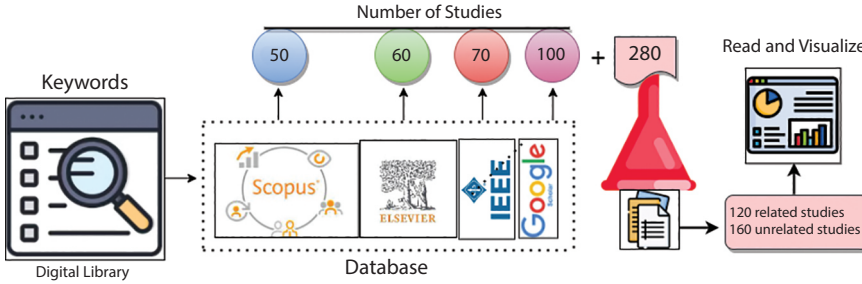

Figure 1.5 Overview of data-collection process flowchart.

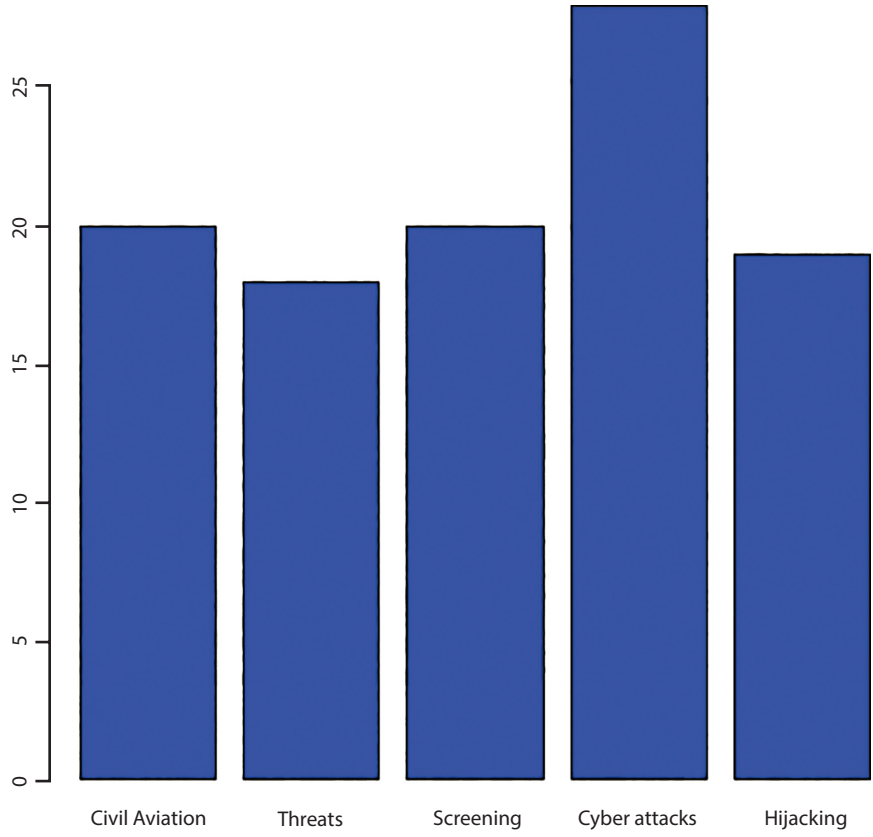

Figure 1.6 Overview of the related studies problems.

the keyword "Civil Aviation, Security Issues and Challenges." We selected these databases because they contain many research papers, book chapters and online information on numerous subjects.

There are 220 studies that have been filtered for problems from 160 unrelated studies. An overview of the studies is shown in Figure 1.6.

1.4 Cyber Risk in Aviation

Cyber risk in aviation is the potential threat that cyberattacks, like those on air traffic control systems, airport security systems, and airline computer networks, could pose to aircraft systems and related infrastructure. More and more computerised systems, like avionics and communication systems, are used in aviation. This has made the industry vulnerable to cyber threats. Cyberattacks on aviation systems can have serious consequences, including losing aircraft control, disrupting air traffic control systems, and compromising sensitive data [37–39]. Cyber threats to aviation can come from various sources, including state-sponsored hackers, criminal organizations, and individual actors. To mitigate the risks associated with cyber threats, stakeholders in the aviation industry have implemented various measures, such as increasing cybersecurity training for employees, implementing more secure systems, and collaborating with cybersecurity experts to [40–42] detect and prevent attacks. Additionally, government agencies have established regulations and guidelines to ensure the safety and security of aviation systems. Companies in the aviation industry need to stay on the lookout for cyber threats and keep producing and putting into place effective cybersecurity measures as technology changes and new threats appear. Figure 1.7 shows major cyberattacks by country, 2006-2020.

The repercussions of committing a cybercrime can be devastating. If a hacker undermines national security by breaking into a U.S. government agency, hackers might face up to 20 years in prison. Attacks on an airport's telecommunications service have been commonplace because of its importance to the economy and the difficulty of penetrating its defences. The first attack occurred when a teenager used a known flaw in the system to launch a denial-of-service assault on the airport's network. There have also been remote hacking assaults, with the air traffic control system, airplanes, and airports being primary targets. The assaults raise concerns about passport control, passenger safety, and luggage control [43–45]. One Australian airport is attacked every day by a consultant with CQR Consulting. The European Aviation Agency estimates that around 1,000 hacks happen in

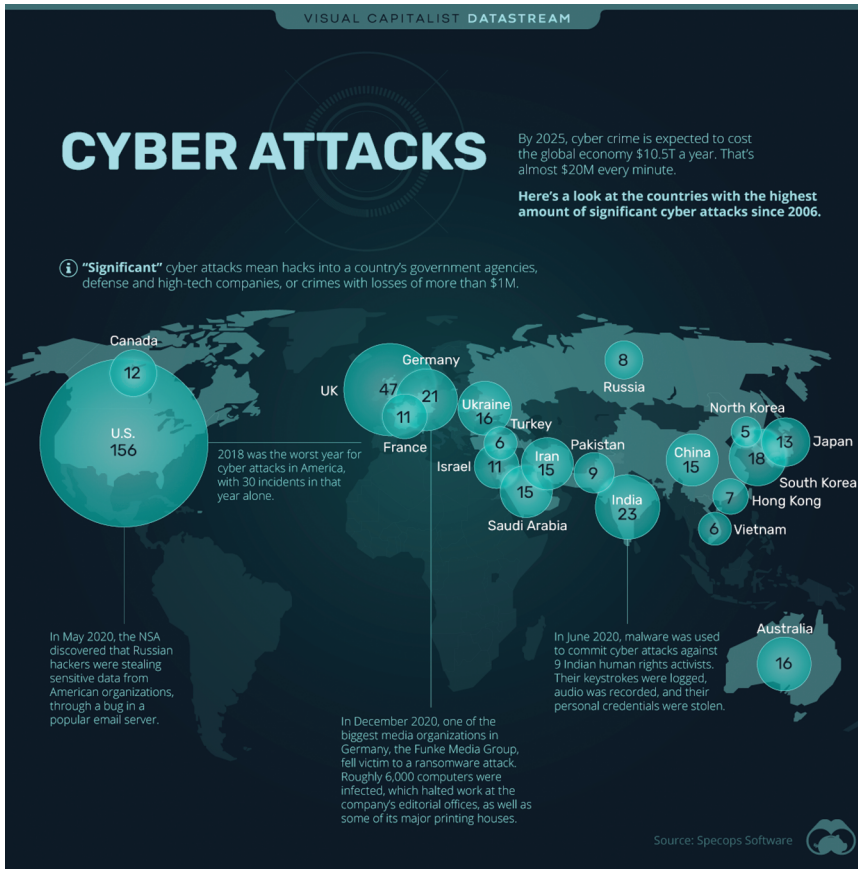

Figure 1.7 Major cyberattacks by country, 2006-2020 [77].

airports every month. A hacker from Tunisia breached a U.S. airport's computer and communication systems in 2014. LOT, a Polish airline, had an attack on its airport's flight operating system due to a distributed denial-of-service attack in 2015. This incident caused the cancellation of roughly 22 flights and forced about 1,400 people to abandon their flights [46–49]. Distributed denial-of-service (DDoS) assaults are frequent in the aviation sector and allow threat actors to disable the system and get access to it. Airports, air buses, air transportation, etc., are all part of the aviation industry's infrastructure. This study suggests that air travel is an essential part of the aviation industry's key infrastructure.

1.4.1 Voice (Very High Frequency – VHF)

The primary method of communication between air traffic control and the plane is via the human voice, known as voice communication. It is used to transmit reports and requests from the aircraft to air traffic control and vice versa. The weather, flight details, and airport-specific updates are just some of the things that are aired. Very high-frequency (VHF) and high-frequency (HF) radios are responsible for this interaction (high frequency). This service is vulnerable to DoS attacks because it relies on a shared frequency for communication between planes and air traffic controllers [50–53]. Several authorities have speculated that the attackers are using unlicensed aviation transceivers or pirate radio stations to target aeroplanes. Spoofing in voice communication has been documented, highlighting the importance of protecting these systems. Attacks like jamming can essentially disable a VHF, leading the plane to use an unauthenticated data channel that is simpler to hack into. VHF intruder detection rates are between 30% and 40%.

1.4.2 Automatic Dependent Surveillance-Broadcast (ADS-B)

Aircraft use this system to transmit data such as their unique identifier, speed, location, and any important messages. The aircraft's identifier is sent out once every five seconds. The position and speed are sent out twice every second. Because of the improved precision of location, this is a crucial application in both European and American airspaces [54–56]. There is no encryption or authentication for sent communications, making this system vulnerable to attack. A researcher called Andrei Costin presented an attack against ADS-B at the Black Hat USA conference. For this assault, he employed an ADS-B receiver to spoof the messages that were being acknowledged by the other receiver, which cost him a total of $1,000 for the software-defined radio. This example proved that these signals are easily intercepted and spoofed by attackers [57]. Attackers can install a replay attack, for instance, to intercept flight data packets and then retransmit them to the targeted system.

1.4.3 Importance of Satellite Navigation (GPS)

The NextGen system, in which the Global Positioning System (GPS) will feature prominently, was recently introduced. GPS has suffered from numerous security flaws since its inception. The feeble transmissions on the single civilian frequency have been shown in research to make GPS

susceptible to hacking. In addition, GPS jammers can be purchased or constructed with little effort. Jamming and other forms of attack against GPS systems can prevent them from getting any signal, leading to poor performance. Deception of pilots and control systems due to spoofing can potentially have severe consequences [58–60]. Radio frequency assaults are a type of serious attack that may inflict harm on both people and their gadgets. Satellite communication is extremely vulnerable to interference since it relies on radio waves to transmit power.

1.5 Distributed Denial of Service (DDoS)

Distributed Denial of Service is referred to as DDoS. It is a kind of cyberattack in which a target system or network is bombarded with an excessive volume of traffic or requests using a number of hacked machines or devices. A DDoS assault aims to stop the target from operating normally and make it inaccessible to authorized users.

1.5.1 Impact of DDoS on Air Transportation

DDoS attacks can have a big effect on air transportation systems, especially on the computer systems and networks of communication that keep the industry running. Several of the above attacks have happened, and it was also found that the aviation industry has many weak spots, making it easy for attackers to get into the fastest-growing industry. A distributed denial-of-service attack was found to be the most common type of attack against aircraft and the systems that support it earlier in the investigation. Websites and other online services are the primary targets of this kind of assault. The goal of this type of assault is to disrupt or slow down the target by sending an excessive amount of traffic to it [61–63]. There are a variety of ways that information might be used inappropriately, from outright destruction of technology to encrypted data held for ransom.

1.6 Discussion

Cybersecurity is becoming increasingly important in the aviation industry due to the growing number of cyberattacks and the increased reliance on technology in aviation systems to ensure civil aviation security. Understanding the aviation system's inner workings is necessary before implementing aviation security. Communication, navigation, and surveillance are the three

primary functions of the aviation system's subsystems and wireless technologies. Airline safety is also a major focus for CNS [64–67]. The airfield serves as a landing spot for planes. It does this with the use of ground stations, satellites, and similar aircraft. Using established communication methods, the pilot exchanges information with the ground station and satellite by voice call or text message. It flies and lands safely thanks to the employment of navigation protocols, the Instrument Landing System (ILS), and Distance Measuring Equipment (DME). To monitor air traffic and look for trespassers, ground control uses surveillance protocols such as primary surveillance radar, secondary surveillance radar, and automatic dependent surveillance broadcast (ADS-B). During take-off, flight, and landing, these systems are always operating. Connectivity in the aviation sector is managed by the Air Traffic Management (ATM) system. So, when connecting with aeroplanes and satellites, the ATM system relies on air traffic control (ATC) as its central hub. With the help of ATC, networks on the ground may communicate with data centres and vice versa. Satellites and other features, such as aeroplane networks, are within the purview of ground networks. Connectivity between ground stations and aeroplanes is vital to the aviation system's operation. Contact with an incoming aircraft is often initiated by the ground station. Connectivity with supplementary ground units is handled by an ATC, which is part of the ground station.

1.6.1 Importance of IoT in Civil Aviation

The Internet of Things (IoT) is a network that enables previously disconnected devices and infrastructure to exchange data and perform tasks together. The IoT offers several potential uses in the aviation industry, including boosting plane efficiency, cutting down on repair bills, and providing a more enjoyable ride for passengers. Aircraft maintenance is one of the most important uses of the IoT in the aviation industry. The engines, landing gear, and avionics are just some of the systems and components that might benefit from being monitored by IoT sensors [68–70]. This information may be analysed in real time, letting maintenance teams see problems before they escalate and plan their work more effectively. By analysing weather and air traffic patterns in real time, IoT may also enhance aircraft performance. Airlines can save money in the long term by using this data to plot more efficient flight patterns that need less fuel. Smart airports are another manner in which the Internet of Things may enhance the travel experience for travellers. With the use of IoT sensors, airports can monitor passenger flow, queue lengths, and wait times. Figure 1.8 shows IoT applications.