



Safeguarding Skies: Airport Cybersecurity in the Digital Age

Suphannee Sivakorn*, Nuttaya Rujiratanapat*, Yotsapat Ruangpaisarn*,
Chanond Duangpayap* and Sakulchai Saramat*

Received: March 6, 2024
Revised: November 16, 2024
Accepted: November 25, 2024

* Corresponding Author: Suphannee Sivakorn, E-mail: suphannee_si@rmutto.ac.th

DOI: 10.14416/j.it/2025.v2.005

Abstract

The aviation industry faces significant vulnerabilities from both physical and cybersecurity threats, highlighting the urgent need for enhanced cybersecurity measures amid increasingly sophisticated attacks. This paper systematically reviews emerging threats at airports, analyzing real-world incidents and relevant literature while mapping risks to the MITRE ATT&CK Matrix, a widely recognized knowledge base for categorizing cyberattack tactics, techniques, and procedures. This is the first to apply the MITRE Matrix to airport security risks, offering a novel approach to understanding and mitigating these challenges. Building on this analysis, the paper advocates for modern cybersecurity defense models, emphasizing Cybersecurity Frameworks and Zero Trust Architecture, as well as critical measures for supply chain risk management and strategies to mitigate ransomware and DoS attacks. Our analysis provides insights into vulnerabilities and actionable recommendations, serving as a comprehensive guide for aviation stakeholders to strengthen defenses against evolving cybersecurity threats.

Keywords: Airport Cybersecurity, Aviation Cybersecurity, Cyber Threats in Aviation, Critical Infrastructure, Smart Airport.

1. Introduction

In the physical domain, airport security entails the screening of passengers, baggage, cargo, and the fortification of secure areas within the airport premises. Airport authorities undertake substantial efforts to prevent unlawful interference and

ensure their security practices meet current standards. However, in the realm of technology, cybersecurity often receives inadequate attention than physical security, as evidenced by a 2017 survey of the top major airports in Europe and the U.S., wherein only 59% of respondents claimed to have an effective cybersecurity policy [1]. This oversight is concerning, especially given a 530% increase in cyberattacks within the aviation industry from 2019 to 2022 [2]. Recent initiatives by authorities, including the Transportation Security Administration (TSA) and the International Air Transport Association (IATA), emphasize the need for enhanced cybersecurity measures, mandating proactive steps to mitigate cyber threats [3], [4].

In an effort to strengthen the cybersecurity posture of the aviation industry, this study comprehensively explores existing literature and recent data on airport cybersecurity. We examine airport technologies, security concerns, and recent cyber incidents in Section 2, and outline our research methodology in Section 3. Section 4 presents a systematic literature review of airport cybersecurity from the past five years, and Section 5 categorizes the current landscape and identifies relevant risks. We map these risks to the MITRE ATT&CK Matrix for Enterprise, a widely recognized cybersecurity knowledge base for developing effective security strategies in Section 6. Section 7 presents modern cybersecurity defense strategies, advocating for Cybersecurity Frameworks and Zero Trust Architecture and highlights essential measures for mitigating supply chain risks, ransomware, and denial-of-service (DoS) attack. Section 8 discusses key challenges

* Department of Computer Science, Faculty of Science and Technology, Rajamangala University of Technology Tawan-ok

and outlines future research directions in this field, with the conclusion presented in Section 9.

The major contributions of this paper are as follows:

- We conducted an extensive analysis of recent cyberattacks and a literature review from the past five years, categorizing key cybersecurity risks into nine distinct areas to clarify the challenges faced by modern airport operations.
- We correlate these identified risks with the MITRE ATT&CK Matrix for Enterprise, making this paper the first to map airport security risks to the Matrix. This serves as a valuable tool for exploring each risk through practical defenses and best practices outlined in the MITRE knowledge base.
- Based on our analysis, we advocate for adopting modern security practices, including Cybersecurity Frameworks and Zero Trust Architecture, along with practical measures to defend against evolving airport cyber threats.

2. Background

Understanding airport technologies, threat actors, and recent high-profile incidents highlights the need for stronger security measures. This section examines airport technology, cybersecurity concerns, the landscape of cyber threat actors, and notable attack incidents.

2.1 Airport Technology and Security Concerns

Airport operations have transformed significantly to support the global aviation industry growth, leading to advancements in technology aimed at enhancing efficiency and service. The evolution of airport technology is delineated into four stages: Airport 1.0 - 4.0.

Airport 1.0 primarily focuses on ensuring the physical safety of operations, with no security concerns [5].

Airport 2.0 incorporates technologies for collaboration technologies such as IP telephony, broadband, and Wi-Fi [6]. Following the events of 9/11, the TSA was established to oversee transport security [7].

Airport 3.0 or "Smart Airport" integrates the Internet of Things (IoT), Artificial Intelligence, smart sensors to enhance passenger experience [8].

Airport 4.0 emphasizes the use of technologies to support airport operations and enhance passenger experiences, with a focus on data analytics as a core capability [9], [10].

While these airport advancements offer notable benefits, they are susceptible to interference and malicious modification without proper deployment.

2.2 Airport Cyber Threat Actors

Incidents of air terrorism have led adversaries to adapt their tactics in both physical and cyber domains [7]. This section outlines four types of cyber threat actors:

1: Advanced Persistent Threat (APT): Organized groups or foreign governments motivated by political or economic goals. They often target critical infrastructure, including airports [11] - [16].

2: Cybercrime: Attackers in this category target systems for valuable and sensitive information from passengers and airport employees [17] - [21], particularly those that are internet-facing or publicly accessible [17].

3: Peer Group Service Disruption: Hackers motivated by political agendas or beliefs whose focus is on service disruptions rather than data theft and financial gain [22] - [30].

4: Insider Threats: Risks that originate from within the organization, typically associated with current or former members of the organization, it may also arise from third parties such as contractors and temporary workers.

2.3 Recent Notable Cybersecurity Incidents

The urgency of cybersecurity in airports has become apparent through numerous studies [1], [5], [8]. From 2022 to 2024, various notable incidents have highlighted cyberattacks affecting airport operations and public perception. Table 1 details and categorizes these incidents by attack type, including Denial-of-Service, Ransomware, Vulnerability Exploitation, and Phishing. This analysis will assist in identifying cybersecurity risks and associated attack vectors for airports in Section 5.

Denial-of-Service (DoS). Recently, several major U.S. airports were targeted by coordinated DoS attacks [29], which overloaded airport servers. Similar incidents have occurred at various airports worldwide [23] - [31]. In some cases, attackers have demanded cryptocurrency payments to stop the attacks, exploiting the difficulty of tracing such transactions [32].

Ransomware. The airport industry has experienced a significant increase in ransomware attacks, primarily due to system vulnerabilities and phishing attempts [33] - [35], [38]. In 2024, notable incidents led to delays in passenger processing and flight schedules [34], [35], while others resulted in the leakage of sensitive data [33].

Vulnerability Exploitation poses significant risks for airports, which rely on variety of software applications for their operations, ranging from flight scheduling, air traffic control, baggage handling, and security systems [1], [5], [8]. This diversity broadens the attack surface, introducing potential vulnerabilities and inadequate security practices from vendor [17], [19], [20] - [22], [25], [36], [37].

Phishing. Although no new incidents have been disclosed recently, phishing remains a significant threat with airport employees and customers vulnerable to scams [38]. During a recent global outage linked to CrowdStrike [39], opportunistic hackers exploited the situation by sending fake information to scam IT personnel [40].

3. Research Methodology

This study synthesizes recent airport cybersecurity incidents, literature, insights from online sources, and an examination of various cybersecurity standards and policies. Our goal is to identify and delineate the prevailing cybersecurity threats and risks, categorizing them in alignment with the MITRE ATT&CK Matrix. By systematically mapping these risks to the Matrix, we provide a strategic approach for mitigating cybersecurity risks and applying effective defense techniques based on current best practices.

4. Literature Review

We conduct a comprehensive literature review by searching academic databases, including Google Scholar, ResearchGate, Scopus, and Web of Science, using the following keywords: "airport AND cybersecurity", "aviation AND cybersecurity", "airport AND information security", "airport AND IT security", "smart airport", and "airport AND cyber risk". Our focus was on peer-reviewed studies from the last five years addressing the impacts of cybersecurity on modern airports, challenges, and risks, while excluding studies on airport physical security or unrelated aviation topics. In total, we reviewed 31 publications, categorizing them into eight primary areas: (1) Critical Infrastructure, (2) IoT, Smart Devices, and AI Technology, (3) Supply Chain, (4) Cybersecurity Awareness, (5) Risk and Threat Analysis, (6) Standards and Regulations, (7) Cybersecurity Framework, and (8) Case Studies and Surveys. Table 2 presents the number of publications in each category and highlights specific airport security risks where applicable.

Critical Infrastructure. This category focuses on the critical infrastructures of airports, such as communication protocols, Air Traffic Management (ATM), and surveillance technologies [41] - [47]. These studies analyze vulnerabilities and mitigations, with examples including man-in-the-middle attacks between aircraft and ground control [42], the lack of encryption in the Automatic Dependent Surveillance-Broadcast (ADS-B) [43], [45], and the security concerns related to digitization of the Traffic Collision Avoidance System (TCAS) [44]. These findings underscore the need to address cybersecurity risks in airports. To this end, we associate these publications related to airport security risks as follows: (1) Insecure Network Architecture, (2) Malware and Ransomware (3) Data Breach and (4) DoS.

IoT, Smart Devices, and AI Technology. Research here addresses cybersecurity risks from IoT devices and AI technologies used in airport operations [1], [5], [8], [48] - [50]. Consequently, we associate these publications with specific risks, including: (1) Public-facing Access, (2) Insecure Network Architecture, (3) Internet-facing Applications and Services,

Table 1. Summary of Publicly Disclosed Notable Cybersecurity Incidents at Airports (2022-2024).

Attack Incident	Attack Incident Summary	Year	Attack Technique	Impact on Airport Services			Threat Actor Type*
				Operational Disruption	Website or Application	Data Leakage	
Seattle Airport [33]	The Port of Seattle confirmed that a ransomware attack caused significant outages at Seattle-Tacoma International Airport, affecting services like Wi-Fi, check-in kiosks, and passenger displays. The attack also resulted in some data being stolen and encrypted	2024	Ransomware	•		•	2
Pau-Pyre'ne's Airport [34]	Pau-Pyre'ne's Airport was hit by a ransomware attack from the MONTI group, which exfiltrated sensitive data and published it on the dark web.	2024	Ransomware			•	2
Croatia's Split Airport [35]	Split Airport in Croatia experienced a ransomware attack that resulted in flight cancellations and delays. The incident has been linked to the Akira group, which is associated with the Russian-based Conti group.	2024	Ransomware	•			2
Los Angeles International Airport [36]	A hacker group, IntelBroker, exploited the airport's CRM system vulnerability, accessing a database with sensitive information (e.g., private plane owners' full names, emails, CPA numbers)	2024	Vulnerability Exploitation			•	2
Copenhagen Airport [31]	The airport website was taken offline. Passengers were advised to use their smartphones as an alternative to receive updates on their flights.	2024	DoS		•		unknown
Beirut International Airport [17]	Hackers displayed a message on screens at the airport threatening to bomb the airport.	2024	unknown	•			3
Long Beach Airport [18]	Part of Long Beach City system cyberattack. The website was taken offline.	2023	Ransomware		•		2
Cairo International Airport [23]	The airport website and mobile application were taken down. Anonymous Collective hacker group took credit for the attack.	2023	DoS		•		3
Czech and Prague Airport [24]	The airport website was taken offline.	2023	DoS		•		3
Quere'taro Intercontinental Airport [19]	LockBit ransomware hacker group took credit for the attack, threatening to leak data. The airport claimed that stolen data was in the public domain.	2023	Ransomware			•	2
Montreal-Trudeau International Airport [25]	Border checkpoint outages e.g., check-in kiosks and electronic gates caused significant delays. A hacker group, NoName057(16) claimed responsibility.	2023	DoS	•			3
Charles de Gaulle Airport [26]	The airport website was taken offline. Cybercriminal, Dark Storm, claimed responsibility.	2023	DoS		•		3
UK Airports [27]	The airport website was taken offline. UserSec hacker group claimed the responsibility.	2023	DoS		•		3
Kenya Airports Authority [20]	Data breach incident. Attackers released data including procurement plans, physical plans, site surveys, invoices and receipts.	2023	unknown			•	2
German Airports [28]	Several German airports' websites were taken offline.	2023	DoS		•		3
US Major Airports [29]	Coordinated DoS attacks targeted several major US airports. A hacker group, Killnet claimed responsibility.	2022	DoS		•		3
Brazil Airports [37]	Rio de Janeiro airport's electronic displays were hacked to show pornographic movies instead of ads and flight info.	2022	Vulnerability Exploitation	•			unknown
Italian Airports [30]	Coordinated DoS attacks targeted several Italian airports. A hacker group, Killnet claimed responsibility.	2022	DoS		•		3
Swissport at Zurich Airport [21]	Airport ground services and air cargo, Swissport, were hit with a ransomware attack causing Zurich Airport operation disruptions.	2022	Ransomware	•			2

The sign • indicates the impact on airport services from the attack.

*The Threat Actor Type number delineates the category of cyber threat actors in Section 2.2

(4) Malware and Ransomware, (5) Data Breach, and (6) DoS as these threats exploits internet connectivity used by IoT and smart devices. Furthermore, vulnerabilities in these products can lead to supply chain attacks [51].

Supply Chain and Third Party. This category examines cybersecurity vulnerabilities arising from supply chain and third-party partnerships. For example, Hann (2020) emphasized the complex socio-technical landscape of the ATM System [47], emphasizing the need for attention to sectors critical to airport operations, particularly in the context of digital cyber warfare [51], as discussed.

Cybersecurity Awareness. This category investigates the effectiveness of cybersecurity awareness training within airport environments. While numerous studies have highlighted the significance of cybersecurity awareness training [1], [5], [8]. However, only one recent publication by Sabillon et al. (2023) [52] has thoroughly examined this topic. We categorize these publications under the following risks: (1) Social Engineering, (2) Insider Threats, and (3) Data Breach, as these risks often arise from human [1], [5], [8], [52] - [54].

Risk and Threat Analysis. This research category conducts literature reviews to identify risks and threats affecting airports. Studies provide insights into threats and recommend improvements for threat detection and response [41], [43], [49], [55] - [64]. Numerous works study airport cybersecurity incidents [55] - [60], including threat actor typologies [58], [61] and associated risks and threats in relation to ICAO (International Civil Aviation Organization) standards [55], which encompass the entire spectrum of airport security risks.

Standards and Regulations. Publications in this category review existing cybersecurity standards and regulations pertinent to the aviation sectors [63] - [66]. They study challenges and gaps in airport cybersecurity policies posed by rapid technological development and call for international cooperation and standardized policies, which currently remain insufficient [64].

Cybersecurity Framework. This category investigates frameworks tailored for airports, focusing on models that

systematically manage risks and enhance resilience. While many studies agree the necessity of these frameworks [1], [5], [8], [41], [55], [67], [68] for example, adopting the National Institute of Standards and Technology's (NIST) Cybersecurity Framework to comply with ICAO standards [55], only few recent publications [55], [67], [68] provide actionable details. Nevertheless these frameworks often lack comprehensive insights into adversary behavior, which are essential for identifying and responding to threats throughout an attack's lifecycle. Further details will be provided in Section 6.

Case Study and Survey. This category focuses on research examining the cybersecurity posture of specific airports. Publications may present case studies based on geography [60], [62], [63], or specific events [69], [70] like the COVID-19 pandemic [70] to gather insights on cybersecurity practices and challenges.

5. Airport Security Risks

This section provides detailed exploration of cybersecurity risks associated with attack vectors (Section 2.3) and those identified in our literature review (Section 4).

5.1 Public-facing Accesses

BYOD. The practice of Bring-Your-Own-Device (BYOD) commonly raises concern due to the exposure of organizations to vulnerabilities [71], [72]. However, in airport settings, passengers commonly use their personal devices. The diversity of connected devices in this context complicates device management [73], heightening the security risk when these devices connect to airport networks.

Public Access Services such as Wi-Fi access, check-in kiosks, and charging stations enhance the passenger experience [6], but they also increase risks by leaving users vulnerable to cyberattacks [74] - [76], particularly if proper network segmentation is not implemented.

Man-in-the-Middle (MITM) attacks are prevalent on public Wi-Fi, where cybercriminals eavesdrop using network snooping and sniffing tools to steal sensitive information [75], [77]–[79]. Despite this, many critical websites continue to serve content over unencrypted connections [79] - [81].

¹NIST Cybersecurity Framework:
<https://www.nist.gov/cyberframework>

Table 2. Airport Cybersecurity Publications by Category and Associated Security Risks.

Publication Category	List of Publications	Number of Publications	Associated Security Risks (when applicable)
Critical Infrastructure	[41] - [47]	9	Insecure Network Architecture Malware and Ransomware Data Breach DoS
IoT, Smart Devices and AI Technology	[1], [5], [8], [48] - [50]	6	Public-facing Access Insecure Network Architecture Internet-facing Applications and Services Malware and Ransomware Data Breach Supply Chain and Third Party DoS
Supply Chain and Third Party	[47]	1	Supply Chain and Third Party
Cybersecurity Awareness	[52]	1	Social Engineering Insider Threats Data Breach
Risk and Threat Analysis	[41], [43], [49], [55] - [64]	13	Public-facing Access Insecure Network Architecture Internet-facing Applications and Services Social Engineering Malware and Ransomware Data Breach Supply Chain and Third Party Insider Threat DoS
Standard and Regulation	[63] - [66]	4	(inapplicable)
Cybersecurity Framework	[55], [67], [68]	3	(inapplicable)
Case Study and Survey	[60], [62], [63], [69], [70]	5	(inapplicable)
	Total	31	Public-facing Access Insecure Network Architecture Internet-facing Applications and Services Social Engineering Malware and Ransomware Data Breach Supply Chain and Third Party Insider Threat DoS

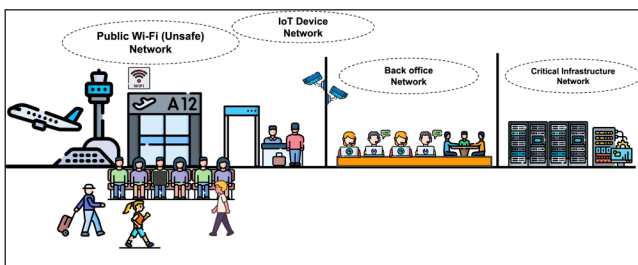


Figure 1. Basic Network Segmentation for Airport Security.

Malware from Untrusted Devices. In this attack, bad actors aim to inject malicious payload onto Wi-Fi users' devices [82], [83]. Adversaries may target vulnerabilities on popular devices, e.g., iOS [84]. Public charging stations also pose risks, known as "juice jacking", where attackers use these stations to spread malware and extract data from smartphones [85].

Malicious Hotspots. A malicious hotspot, also known as a "rogue access point" poses a significant threat to public Wi-Fi users. The attacker sets up a wireless access point with an identical SSID to deceive users, making users vulnerable to MITM or other network attacks [86] - [88].

5.2 Insecure Network Architecture

An insecure network architecture may allow attackers to gain access to internal systems and move laterally across organization assets. Effective network segmentation is a key component, enabling administrators to manage network interactions more securely by implementing security policies, with varying levels of security and trust assigned to different applications [89]. Figure 1 illustrates a basic example of network segmentation applicable to an airport, where each segment

requires specific measures and is separated based on the different entities and stakeholders involved, which can be described as follow:

Public Wi-Fi. To prevent potential malicious activities spreading to other airport entities such as CCTV systems [1] and malware incidents at Vienna Airport [90], it should be completely segregated from other airport networks.

IoT Devices. IoT devices often rely on vendor or third-party-based solutions, making them vulnerable to third-party security risks (Section 5.7). Consequently, it is recommended to isolate them from other networks, particularly critical networks.

Back Office is responsible for the administration, operations and logistics of the airport. Given the human-centric nature of these operations, this network is prone to risks such as phishing, social engineering, and other human errors. This network should be kept separated for added security.

Critical Infrastructures includes crucial assets for the airport operations. Access to this network should be restricted from the public network, robust authentication and encryption measures must be implemented, as highlighted in several studies discussed in Section 4.

5.3 Internet-facing Applications and Services

Security Vulnerabilities. Adversaries often exploit weaknesses in internet-facing applications such as airport websites, and mobile applications. These vulnerabilities can arise from software bugs, design flaws, or unpatched vulnerabilities, as discussed in Section 2.3 and Section 4.

Weak authentication practices in internet-facing applications pose significant risks for airports, potentially leading to unauthorized access to critical systems. Additionally, remote access for employees can further complicate security; if authentication credentials are weak, attackers may gain broader access to internal networks [91].

5.4 Social Engineering

Phishing. Social engineering attacks exploit human vulnerabilities, with phishing being a significant concern. In 2013, over 75 U.S. airports reported incidents involving

phishing emails designed to deceive users into disclosing financial information [61]. Some of these attacks predominantly target employees with privileged access to critical systems [8].

5.5 Malware and Ransomware

Ransomware incidents often lead to airport operational disruptions and passenger experience [18], [19], [21], [33] - [35]. Additionally, malware attacks may lead to data breaches, exposing sensitive information such as passenger records, payment details, and employee credentials [31], [32]. Such breaches jeopardize privacy and can incur financial costs for airports, including remediations and regulatory fines.

5.6 Data Breach

Data breaches often results in the unauthorized access, disclosure, or theft of sensitive information [19], [20], [33], [34], [36]. Additionally, breaches of sensitive operational information can undermine airport operations and lead to security vulnerabilities [20]. In some cases, attackers may exfiltrate data and demand ransom for its return or for the decryption of compromised systems [32].

5.7 Supply Chain and Third-Party

Security Vulnerabilities in systems can allow attackers to gain unauthorized access. These weaknesses may stem from known or unknown third-party software and hardware bugs, and misconfigurations [92]. Zero-day vulnerabilities pose particular risks, as attacks can occur before developers issue patches. Concerns about IoT and vendor solution vulnerabilities are amplified by the potential for threat actors to compromise not only the affected device but also other network assets [93].

No Security Update Mechanism. Many solutions, particularly IoT devices, may lack a security update mechanism, leaving them vulnerable even after patches have been released [94].

No Common Standards and Specifications. The lack of universally accepted standards for IoT device development leads to inconsistent implementations and design choices, which negatively affect security. Users must manage multiple technologies to effectively support these devices [5].

Supply Chain Compromise involves manipulating products

before they reach consumer, creating vulnerabilities in critical systems. For example, compromised chips or drivers in smart devices at airports can expose systems to attack [95]. High-profile incidents, such as the SolarWinds hack, affected over 18,000 networks globally [96]. Additionally, a recent incident in Lebanon further illustrates the dangers, where devices were reportedly manipulated for digital warfare [51].

No Physical Hardening. IoT devices are often deployed in various locations throughout the airport, making them vulnerable to tampering during unattended operations. Physical access can result in theft and unauthorized access to internal circuits and overwriting changes [1].

5.8 Insider Threat

An insider threat is a security risk posed by individuals who misuse their access or privileged accounts. A malicious insider, often referred to as a "Turncloak," intentionally abuses legitimate access to steal sensitive information or manipulate critical aviation systems. Mitigating this threat involves adhering to information security management standards and guidelines [97].

5.9 Denial-of-Service

As outlined in Section 2, DoS attacks on airport websites are significant threats to the aviation sector, with recent trends showing demands ransom payments to stop these attacks, aided by the anonymity of cryptocurrencies [32].

6. Airport Security Risks and MITRE ATT&CK Matrix

This section provides a comprehensive analysis of the security risks faced by airports, categorizing these risks in alignment with the MITRE ATT&CK Matrix for Enterprise (or MITRE Matrix) [98]. This widely adopted cybersecurity knowledge base outlines the tactics, techniques and procedures (TTPs) utilized globally for threat analysis and security defenses. Notably, this paper is the first to propose applying the MITRE Matrix to bolster the cybersecurity posture of airports. We correlate all identified airport security risks—derived from cybersecurity incidents and a systematic literature review—with MITRE techniques to mitigate cyberattacks

arising from these identified risks.

6.1. MITRE Matrix: TTPs

The MITRE Matrix categorizes attacker tactics and techniques. Each tactic represents a high-level goal, while the techniques describe the specific methods employed to achieve that goal, both indexed for easy reference. Each technique includes (1) procedures based on real-world incidents, (2) mitigations with actionable defense recommendations such as configurations and tools, and (3) detection strategies and recommendations for identifying the attacks. We believe that this comprehensive information enables airport security personnel to effectively implement strategies to mitigate identified risks.

6.2 Airport Security Risks with the MITRE Matrix

The MITRE Matrix is a valuable tool for identifying and mapping airport security risks related to potential attacks. Given the complexity of vulnerabilities, some risks may align with multiple MITRE techniques. This paper focuses on two key tactics: Initial Access (TA001) and Impact (TA0040). Initial Access is fundamental as it represents the first step for adversaries to gain entry into protected systems. The Impact tactic, particularly T1498 (Network Denial of Service), is emphasized due to its prevalence due to its frequency in recent incidents discussed in Section 2.3.

Table 3 provides an overview of categorized airport security risks and their associated MITRE techniques, listing all ten Initial Access techniques and one Impact technique (retrieved September 2024). Each technique is identified and referenced by an ID (e.g., T1189, T1190).

6.3 MITRE Initial Access Techniques (TA0001)

Initial Access is a critical phase in the cyber kill chain, representing the methods adversaries use to gain entry into target systems. Below are the relevant techniques from the MITRE Matrix associated with Initial Access and the corresponding airport security risks:

Public-facing Access (T1659, T1190, T1200): Techniques such as Content Injection (T1659) allow attackers to insert malicious content into network traffic, often through public Wi-Fi. Exploiting vulnerabilities in public-facing applications (T1190),

² MITRE Matrix Initial Access Tactic:
<https://attack.mitre.org/tactics/TA0001/>

³ MITRE Matrix Impact Tactic:
<https://attack.mitre.org/tactics/TA0040/>

Table 3. Summary of Airport Security Risks Linked to MITRE Matrix Tactics and Techniques.

Airport Security Risk	Initial Access: TA0001										Impact: TA0040
	T1659	T1189	T1190	T1133	T1200	T1566	T1091	T1195	T1199	T1078	T1498
1. Public-facing Accesses	•		•		•						
2. Insecure Network Architecture	•		•	•							
3. Internet-facing Applications and Services			•	•							
4. Social Engineering Attacks	•	•				•	•			•	
5. Malware and Ransomware	•	•	•	•	•	•	•	•	•	•	
6. Data Breach	•	•	•	•	•	•	•	•	•	•	
7. Supply Chain and Third Party				•	•			•	•		
8. Insider Threats							•		•	•	
9. DoS											•

The sign • indicates that the airport security risk shown can be categorized according to the specific MITRE Matrix technique.

Associated MITRE Initial Access Tactic (TA0001)

ID	Technique
T1659	Content Injection
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
T1091	Replication Through Removable Media
T1195	Supply Chain Compromised
T1199	Trusted Relationship
T1078	Valid Accounts

Associated MITRE Impact Tactic (TA0040)

ID	Technique
T1498	Network Denial of Service

such as kiosks and charging stations, can provide unauthorized access due to unpatched vulnerabilities or misconfigurations. This may be coupled with Hardware Additions (T1200), where attackers exploit exposed ports to introduce unauthorized devices [99].

Insecure Network Architecture (T1659, T1190, T1133):

Techniques such as Content Injection (T1659) and Exploiting Public-facing Applications (T1190) become more dangerous in poorly secured environments, allowing attackers to gain initial access and subsequently move laterally. Additionally, External Remote Services (T1133) may compromise internal network by enabling unauthorized access through insecure remote connections.

Internet-facing Applications and Services (T1190, T1133):

The presence of internet-facing applications and services exposes airports to significant cybersecurity risks via techniques such as Exploiting Public-facing Applications (T1190) and External Remote Services (T1133). Attackers can target vulnerabilities within publicly accessible systems—like online booking websites and service APIs—to gain unauthorized access to sensitive assets. Insecure remote services can also create entry points for attackers, allowing them to gain unauthorized access to internal systems through airport VPNs [100].

Social Engineering (T1659, T1189, T1566, T1091, T1078):

Techniques such as Content Injection (T1659), Drive-by Compromise (T1189), and Phishing (T1566) are utilized to manipulate victims. The use of insecure removable media (T1091) may allow untrusted devices to introduce malware to critical systems [101]. Technique like Valid Accounts (T1078) may enable attackers to gain access via stolen account.

Malware, Ransomware and Data Breach (T1659, T1189, T1190, T1133, T1200, T1566, T1091, T1195, T1199, T1078): Malware, ransomware, and data breaches exploit various techniques within airport systems. Initial Access tactics, such as Content Injection (T1659) and Exploiting

Public-facing Applications (T1190) enable attackers to infiltrate via public interfaces. Techniques like Drive-by Compromise (T1189), Phishing (T1566), and the use of insecure removable media (T1091) increase the risk of malware and ransomware, ultimately leading to data breaches. External Remote Services (T1133) and Valid Accounts (T1078) allow attackers to leverage stolen credentials to penetrate into the networks, facilitating ransomware and data theft. Risks from Supply Chain Compromise (T1195) and Trusted Relationship (T1199) may introduce vulnerabilities into overall security.

Supply Chain and Third Party (T1195, T1199): With multiple party involved, techniques such as Supply Chain Compromise (T1195) and Trusted Relationship (T1199) presents significant threat to airports, allowing attackers to exploit vulnerabilities without raising immediate suspicion.

Insider Threat (T1091, T1199, T1078): Techniques such as Insecure Removable Media (T1091) can enable employees to introduce malware into the system. Exploitation of Trusted Relationships (T1199) may allow insiders to manipulate external connections, leading to unauthorized sharing of sensitive information. Additionally, Valid Accounts (T1078) could allow insiders to misuse their credentials.

6.4 MITRE Impact (TA0040) for Denial-of-Service

Denial-of-Service (T1498): According to the MITRE framework, DoS attacks fall under the Impact tactic, specifically technique ID T1498. This can be executed through methods such as direct network floods (T1498.001) or reflection amplification (T1498.002).

7. Modern Defenses for Airport Security

In this section, we outline modern security defense strategies and best practices specifically designed for airport. The key focus areas include the adoption of Cybersecurity Frameworks and the implementation of Zero Trust Architecture, along with additional defenses addressing the identified risks in previous sections.

7.1 Cybersecurity Frameworks and Requirements

Numerous studies emphasize the important of adopting cybersecurity frameworks to enhance airport security [1], [5], [8], [41], [55], [67], [68]. Frameworks, such as NIST Cybersecurity Framework, can help identify weaknesses and facilitate development of security objectives. The Civil Air Navigation Services Organization (CANSO) has proposed guidelines to elevate security levels through these frameworks [102], and several airports, including Airports of Thailand, have already implemented such policies [103].

Recently, the TSA issued new cybersecurity requirements, mandating all U.S. airports and aircraft operators to develop cybersecurity policies [104], [105]. Additionally, ICAO has created Standards and Recommended Practices [106], [107] that urge airports to implement cybersecurity risk management frameworks and collaborate to advance ICAO's cybersecurity framework.

7.2 Zero Trust Architecture

Zero Trust is a modern cybersecurity framework that prioritizes verifying and protecting all entities based on the principle of least privilege. It involves capturing and analyzing logs for effective threat response, acknowledging that internal threats may stem from untrusted devices and personnel. The following discussion highlights the benefits of implementing Zero Trust architecture in airport security.

Visibility for Subsystems. The initial phase of an integrated Zero Trust architecture involves identifying organizational assets, their value, stakeholders, and connectivity. This foundational step prioritizes Zero Trust security policies, including secure access, the principle of least privilege, and enhanced visibility into subsystems.

Network Segmentation. Network segmentation is a foundational element of the Zero Trust architecture, allowing network administrators to enforce the principle of least privilege. For instance, the IoT network is isolated from other segments to prevent unauthorized parties from exploiting IoT vulnerabilities and mitigate the risk of lateral movement within the airport's infrastructure.

Demilitarized Zone. Internet-based services are prime targets for cyberattacks, making it essential to configure a separate network segment called a "Demilitarized Zone" (DMZ). The DMZ acts as a controlled gateway between the internal network and the internet, enforcing strict connectivity rules through firewalls and packet filtering.

The External Policy Enforcement Point (PEP) in Figure 2 filters malicious internet traffic, while the Internal PEP manages the traffic between DMZ servers and the internal network. This layered security approach ensures that external services remain isolated from internal systems.

7.3 Security Awareness Training. The aviation sector may soon face regulatory mandates requiring security awareness training for employees [4], [7]. To effectively implement such programs, organizations actively engage in the development process, providing continuous feedback to enhance the training effectiveness.

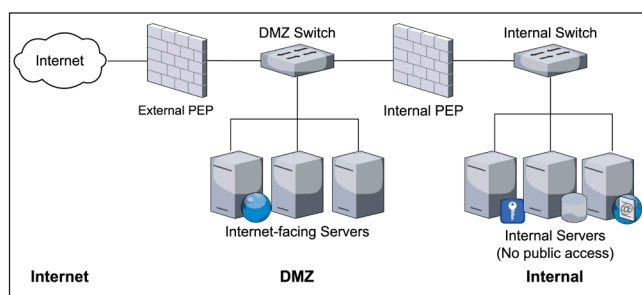


Figure 2. DMZ subnet that separates an enterprise internal network from other untrusted networks e.g., the Internet.

7.4 Malware, Ransomware and Data Breach

In addition to previously discussed security measures, airports should implement targeted strategies to detect malware and ransomware. The following mitigation strategies can strengthen an airport's cybersecurity posture:

Endpoint Detection and Response (EDR). To bolster cybersecurity, airports should implement advanced anomaly detection and monitoring to swiftly identify unusual patterns indicative of ransomware. EDR solutions provide real-time analysis of host activities, enabling rapid detection of malicious behaviors [108].

Data Backup and Disaster Recovery. It is imperative to implement comprehensive IT disaster recovery plans that

encompass regular off-site data backups. These backups must be secured against common threats, such as ransomware that seeks to compromise backup files (T1486) [109]. Routine testing of backup restoration procedures is crucial to ensure their usability in the event of an incident.

Data Breach Prevention involves proactive monitoring of data for irregular patterns—such as unexpected changes in data size, unusual timestamps, or unauthorized access attempts—is essential for early detection of potential breaches. Strong authentication and encryption for data access further safeguard sensitive information from unauthorized users and ensure compliance with relevant regulatory data security and privacy requirements.

7.5 Supply Chain and Third Party Risk Management

Due Diligence in Supply Chain Management.

Any third-party solutions integrated into airport systems must be treated as part of the airport's threat landscape. A rigorous selection process should assess adaptability, security features, secure update mechanisms, and support systems to effectively manage security liabilities and reduce the risk of unforeseen incidents.

Physical Access Restrictions and Tamper Proofing.

IoT devices deployed throughout airports are susceptible to physical access attacks, where criminals may steal them for unauthorized entry. To mitigate this risk, various tamper-proof techniques can be applied [110], [111]. For instance, devices can be housed in secure or tamper-resistant cases and disabling or factory resetting.

7.6 Insider Threat Mitigation

Mitigating insider threats is challenging, as they often bypass traditional security measures. Prevention relies on the principle of least privilege, restricting user access to essential functions, along with monitoring for anomalous behaviors. Implementing a Zero Trust Architecture strengthens security by requiring identity verification for every access request and ensuring all access is logged and analyzed.

7.7 Denial-of-Service Mitigation

Cloud or Hybrid DoS Scrubbing Platforms enhance security by redirecting traffic through specialized infrastructure

that filters out malicious traffic before it reaches the airport's network [112], [113]. Incorporating redundancy and failover mechanisms is also essential, as it improves resilience and minimizes downtime, ensuring essential services remain operational during an attack.

7.8 Collaborative Threat Intelligence Sharing

Numerous studies underscore the importance of information sharing within the industry [5], [61], [64], [114]. A real-world example demonstrates the effectiveness: during a spear phishing campaign targeting airport executives, emails containing malware were detected. Through collaborative efforts, the attack was neutralized across the sector [115]. By adopting a multi-faceted approach, including collaborative threat intelligence sharing, airports can enhance their defenses against evolving cyber threats.

8. Challenges and Future Research Directions

While a range of defenses have been detailed, significant challenges remain that must be addressed in order to further enhance airport cybersecurity

Evolving Threat Landscape. Cyber threats are continuously evolving and becoming more sophisticated, and diversified. This necessitates ongoing research and airport adaptability to counter new attack vectors.

Resource Constraints. Smaller airports often face significant resource limitations e.g., budget and personnel, hindering the implementation of cybersecurity measures.

Integration of Legacy Systems. Integrating modern security measures with outdated systems presents significant challenges and often requires substantial investment.

Future Research Directions. Our literature review reveals a pressing need for further research in key areas: (1) Supply Chain and Third-Party Risks, (2) Cybersecurity Awareness, and (3) Development of Airport-Specific Cybersecurity Frameworks. The limited publications in these domains highlight the unique challenges airports face.

Additionally, future research should investigate the integration of advanced technologies like Machine Learning, AI, and

Generative AI, focusing on their effectiveness in enhancing airport operations while mitigating potential vulnerabilities. While existing studies have started to address these gaps, ongoing research is essential to keep up with emerging threats and solutions.

9. Conclusion

This paper explores the critical area of airport cybersecurity, highlighting the seriousness of emerging threats in this domain. Through insights gained from recent real-world incidents and a systematic literature review, we conducted a comprehensive analysis and categorized major cybersecurity risks confronting airports, aligned with the MITRE ATT&CK Matrix, providing a valuable framework for exploring practical defenses and best practices articulated in the MITRE knowledge base.

In conclusion, we advocate for the adoption of modern security policies, including robust Cybersecurity Frameworks and Zero Trust Architecture, alongside critical security measures. This study aims to enhance the aviation industry's understanding of the current threat landscape and provide a foundation for enhancing cybersecurity defense and resilience.

10. References

- [1] G. Lykou, A. Anagnostopoulou, and D. Gritzalis. "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls." *Sensors*, Vol. 19, No. 1, 2019.
- [2] EUROCONTROL, *Aviation under Attack from a Wave of Cybercrime*. Available Online at <https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cyber-crime>, accessed on 1 February 2024.
- [3] Business Insurance, *US to add cybersecurity requirements for critical aviation systems*. Available Online at <https://www.businessinsurance.com/article/20221012/NEWS06/912353045/US-to-add-cybersecurity-requirements-for-critical-aviation-systems>, accessed on 1 February 2024.

- [4] IATA, *Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation Edition 3.0*. Available Online at <https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a935e278b/compilation-of-cyber-regulations-standards-and-guidance3.0.pdf>, accessed on 1 February 2024.
- [5] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke. "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports." *IEEE Access*, Vol. 8, pp. 209802-209834, 2020.
- [6] A. Fattah, H. Lock, W. Buller, and S. Kirby. *Smart Airports: Transforming Passenger Experience to Thrive in the New Economy*. Available Online at https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf, accessed on 1 February 2024.
- [7] TSA, *20 years after 9/11: The state of the transportation security administration*. Available Online at <https://shorturl.at/1lsGo>, accessed on 1 February 2024.
- [8] G. Lykou, A. Anagnostopoulou, and D. Gritzalis. "Implementing Cyber Security Measures in Airports to Improve Cyber Resilience." *Proceedings of the 2018 Global Internet of Things Summit*, pp. 1-6, 2018.
- [9] J. H. Tan and T. Masood. "Adoption of Industry 4.0 Technologies in Airports - A Systematic Literature Review." *ArXiv*, pp. 1-25, 2021.
- [10] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and E. S. Gonzalez. "Understanding the Adoption of Industry 4.0 Technologies in Improving Environmental Sustainability." *Sustainable Operations and Computers*, Vol. 3, pp. 203 - 217, 2022.
- [11] K. Gopalakrishnan, M. Govindarasu, D. Jacobson, and B. M. Phares. "Cyber Security for Airports." *International Journal for Traffic and Transport Engineering (IJTTE)*, Vol. 3, No. 4, pp. 365-376, 2013.
- [12] Bloomberg, *Colonial Pipeline Cyber Attack: Hackers Used Compromised Password*. Available Online at <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>, accessed on 1 February 2024.
- [13] CNN, *Ransomware attack hits New Jersey county*. Available Online at <https://www.cnn.com/2022/05/26/politics/new-jersey-somerset-county-ransomware-attack>, accessed on 1 August 2023.
- [14] Threatpost, *N.J.'s Largest Hospital System Pays Up in Ransomware Attack*. Available Online at <https://threatpost.com/ransomware-attack-new-jersey>, accessed on 1 February 2024.
- [15] Mandiant, *Advanced Persistent Threats (APTs) -- Threat Actors & Groups*. Available Online at <https://www.mandiant.com/resources/insights/apt-groups>, accessed on 1 June 2023.
- [16] ZDNET, *Russian state hackers behind San Francisco Airport Hack*. Available Online at <https://www.zdnet.com/article/russian-state-hackers-behind-san-francisco-airport-hack/>, accessed on 1 February 2024.
- [17] Security Affairs, *A Cyber Attack Hit The Beirut International Airport*. Available Online at <https://securityaffairs.com/157079/hacking/cyber-attack-hit-beirut-international-airport.html>, accessed on 1 February 2024.
- [18] Homeland Security Today, *Long Beach Airport's Website Taken Down By Cyber Attack*. Available Online at <https://www.hstoday.us/subject-matter-areas/transportation/long-beach-airports-website-taken-down-by-cyber-attack/>, accessed on 1 June 2023.
- [19] The Record, *Major Mexican airport confirms experts are working to address cyberattack*. Available Online at <https://therecord.media/queretaro-international-airport-mexico-cyberattack>, accessed on 1 February 2024.
- [20] NTV, *KAA confirms data breach, says no sensitive data leaked*. Available Online at <https://ntvkenya.co.ke/news/kaa-confirms-data-breach-says-no-sensitive-data-leaked/>, accessed on 1 May 2023.
- [21] Airport Technology, *Ransomware attack on Swissport*

- causes delay at Zurich Airport*. Available Online at <https://www.airport-technology.com/news/ransomware-attack-swissport-zurich-airport/>, accessed on 1 February 2024.
- [22] Security Affairs, *A Cyber Attack Hit The Beirut International Airport*. Available Online at <https://securityaffairs.com/157079/hacking/cyber-attack-hit-beirut-international-airport.html>, accessed on 1 February 2024.
- [23] The Cyber Express, *DDoS Cyberattack Hits Cairo International Airport: Anonymous Collective Claims Responsibility*. Available Online at <https://thecyberexpress.com/cairo-international-airport-cyberattack>, accessed on 1 February 2024.
- [24] Czech Police, *Interior Ministry, Airport Websites Come Under Cyber Attack*. Available Online at <https://brnodaily.com/2023/10/24/news/czech-police-interior-ministry-airport-websites-come-under-cyber-attack/>, accessed on 1 February 2024.
- [25] The Record, *Canada blames border checkpoint outages on cyberattack*. Available Online at <https://therecord.media/canada-border-checkpoint-outages-ddos-attack-russia>, accessed on 1 May 2023.
- [26] Tech Monitor, *Charles de Gaulle Airport website offline after suspected 'OpFrance' DDoS cyberattack*. Available Online at <https://techmonitor.ai/technology/cybersecurity/opfrance-cyberattack-charles-de-gaulle-airport>, accessed on 1 June 2023.
- [27] Mirror, *UK airports targeted by coordinated Russia cyberattack groups*. Available Online at <https://www.mirror.co.uk/travel/news/uk-airports-targeted-coordinated-russia-30504938>, accessed on 1 February 2024.
- [28] Information Week, *The DDoS Attack on German Airport Websites and What IT Leaders Can Learn*. Available Online at <https://shorturl.at/7ACXL>, accessed on 1 February 2024.
- [29] The Associated Press, *Denial-of-service attacks knock US airport websites offline*. Available Online at <https://apnews.com/article/technology-business-atlanta-680cf93f7eb0300127448c35299ad66e>, accessed on 1 February 2024.
- [30] Euractiv, *Italy target of major Russia-linked cyberattack, again*. Available Online at <https://shorturl.at/Kvn9C>, accessed on 1 February 2024.
- [31] CyberMaterial, *Cyberattack Hit Copenhagen Airport*. Available Online at <https://cybermaterial.com/cyberattack-hit-copenhagen-airport/>, accessed on 1 February 2024.
- [32] The Wall Street Journal, *Why Hackers Use Bitcoin and Why It Is So Difficult to Trace*. Available Online at <https://www.wsj.com/articles/why-hackers-use-bitcoin-and-why-it-is-so-difficult-to-trace-11594931595>, accessed on 1 February 2024.
- [33] SecurityWeek, *Data Stolen in Ransomware Attack That Hit Seattle Airport*. Available Online at <https://www.securityweek.com/data-stolen-in-ransomware-attack-that-hit-seattle-airport>, accessed on 1 February 2024.
- [34] Halcyon Tech, *Monti Ransomware Attack on Aéroport de Pau*. Available Online at <https://ransomwareattacks.halcyon.ai/attacks/monti-ransomware-attack-on-aeroport-de-pau>, accessed on 1 February 2024.
- [35] BARRON'S, *Cyberattack Hits Croatia's Split Airport*. Available Online at <https://www.barrons.com/news/cyberattack-hits-croatia-s-split-airport-dac3d776>, accessed on 1 February 2024.
- [36] HACKREAD, *Hackers Leak 2.5M Private Plane Owners' Data Linked to LA Intl. Airport Breach*. Available Online at <https://hackread.com/hackers-leak-private-plane-owners-data-la-airport-breach/>, accessed on 1 August 2024.
- [37] AP, *Hacked Brazil Airport Screens Show Porn to Travelers*. Available Online at <https://apnews.com/article/entertainment-caribbean-brazil-c0842e915c403c418306433cdfc406a6>, accessed on 1 February 2024.

- [38] KTSM.com, *FBI warns cyber criminals are spoofing airport websites and Wi-Fi*. Available Online at <https://shorturl.at/vJRE7>, accessed on 1 February 2024.
- [39] The New York Times, *Stranded in the CrowdStrike Meltdown: 'No Hotel, No Food, No Assistance'*. Available Online at <https://www.nytimes.com/2024/09/13/travel/crowdstrike-outage-delta-airlines.html>, accessed on 1 February 2024.
- [40] BCC, *Scam warning as fake emails and websites target users after outage*. BBC. Available Online at <https://www.bbc.com/news/articles/cq5xy12pyny>, accessed on 1 February 2024.
- [41] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo. "Cyber Security Challenges in Aviation Communication, Navigation, and Surveillance." *Computers & Security*, Vol. 112, 2022.
- [42] E. Andreev and D. Dimitrov. "Analysis of Cyber Vulnerabilities in Civil Aviation and Recommendations for Their Mitigation." *Aeronautical Research and Development*, Vol. 1, pp. 90-99, 2022.
- [43] A. Elmarady and K. Rahouma. "Studying Cybersecurity in Civil Aviation, including Developing and Applying Aviation Cybersecurity Risk Assessment." *IEEE Access*, Vol. 4, 2016.
- [44] M. L. Salgado and M. S. de Sousa. "Cybersecurity in Aviation: The STPASEC Method Applied to the TCAS Security." *2021 10th Latin-American Symposium on Dependable Computing (LADC)*, Florianópolis, Brazil, pp. 1-10, 2021.
- [45] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen. "Cybersecurity Attacks on Software Logic and Error Handling within ADS-B Implementations: Systematic Testing of Resilience and Countermeasures." *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 58, No. 4, pp. 2702-2719, 2022.
- [46] A. A. Alsulami and S. Zein-Sabatto. "Resilient Cybersecurity Approach for Aviation Cyber-physical Systems Protection against Sensor Spoofing Attacks." *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, NV, USA, pp. 565-571, 2021.
- [47] J. Haan. "Specific Air Traffic Management Cybersecurity Challenges: Architecture and Supply Chain." *ICSEW'20: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, New York, NY, USA, pp. 245-249, 2020.
- [48] C. Aranzazu-Suescun, L. F. Zapata-Rivera, O. G.-M. Saenz, and J. M. Christensen. "Securing IoT Surveillance Airport Infrastructure." *Proceedings of the 2024 International Conference on Smart Applications, Communications and Networking*, Harrisonburg, VA, USA, pp. 1-7, 2024.
- [49] E. Pik. "Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience." *Journal of Transportation Security*, Vol. 17, No. 1, December, 2024.
- [50] D. Shevchuk and I. Steniakin. "A Holistic Approach to Ensuring Safety and Cybersecurity in the Use of Intelligent Technologies in Air Transport." *Electronics and Control Systems*, Vol. 1, No. 75, pp. 97-101, 2023.
- [51] The Wall Street Journal, *Pager Attacks in Lebanon 'Weaponize' Supply Chains*. Available Online at <https://www.wsj.com/articles/pager-attacks-in-lebanon-weaponize-supply-chains-60722390>, accessed on 1 February 2024.
- [52] R. Sabillon and J.R.B. Higuera. "The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities." *International Conference on Human-Computer Interaction*, pp. 461-479, 2023.
- [53] S. Chockalingam, E. Nystad, and C. Esnoul. "Capability Maturity Models for Targeted Cyber Security Training." *Proceedings of the International Conference on Human-Computer Interaction*, pp. 576-590, 2023.

- [54] The Hacker News, *Why Human Error is #1 Cyber Security Threat to Businesses in 2021*. Available Online at <https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html>, accessed on 1 February 2024.
- [55] P. Stastny and A. M. Stoica. "Protecting Aviation Safety Against Cybersecurity Threats." *IOP Conference Series: Materials Science and Engineering*, Vol. 1226, No. 1, pp. 12-25, 2022.
- [56] H. Saada, R. Orizio, and S. Sebastio. "Modeling and Conducting Security Risk Assessment of Smart Airport Infrastructures with SECRA." *Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security*, No. 59, pp. 1-7, 2024.
- [57] T. Jeeradist. "Flight Delays and Cancellations Due to Airport Technology Network Disruptions Worldwide." *KBU Journal of Aviation Management: KBUJAM*, Vol. 2, No. 1, pp. 51-60, 2024.
- [58] L. Florido-Benítez. "The Types of Hackers and Cyberattacks in the Aviation Industry." *Journal of Transportation Security*, Vol. 17, No. 13, 2024.
- [59] H. Su and W. Pan. "Using Digital Twins to Integrate Cyber Security with Physical Security at Smart Airports." *Interdisciplinary Journal of Engineering and Environmental Sciences*, Vol. 10, No. 1, pp. 38-45, January-March, 2023.
- [60] S. Samuri, M.F.A. Khir, Z.M. Amin, and M. F. N. Mohammad. "Cybersecurity Maturity Framework for International Airports in Malaysia: A Systematic Literature Review (SLR)." *Journal of Information and Knowledge Management (JIKM)*, Vol. 2, pp. 156-167, 2023.
- [61] E. Ukwandu, M. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andonovid, and X. Bellekens. "Cybersecurity Challenges in Aviation Industry: A Review of Current and Future Trends." *Information*, Vol. 13, No. 3, 2022.
- [62] L.F. Benítez. "Identifying Cyber Security Risks in Spanish Airports." *Cyber Security: A Peer-Reviewed Journal*, Vol. 4, No. 3, pp. 267-291, 2021.
- [63] M. Karpiuk and M. Kelemen. "Cybersecurity in Civil Aviation in Poland and Slovakia." *Cybersecurity and Law*, Vol. 8, No. 2, pp. 70-83, 2022.
- [64] C. Nobles, D. Burrell, and T. Waller. "The Need for a Global Aviation Cybersecurity Defense Policy" *Land Forces Academy Review*, Vol. 27, No. 1, pp. 19-26, March 2022.
- [65] V. Filinovich and Z. Hu. "Aviation and the Cybersecurity Threats." *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)*, pp. 120-126, 2021.
- [66] M. Klenka. "Aviation Cyber Security: Legal Aspects of Cyber Threats." *Journal of Transportation Security*, Vol. 14, No. 3, pp. 177-195, December, 2021.
- [67] S. Adhikari and S. Mirchandani. "Integrating Risk Assessment Modeling with Aviation Cybersecurity Framework." *AIAA AVIATION 2020 FORUM*, pp. 29-32, 2020.
- [68] S. Adhikari. "An Analysis of AIAA Aviation Cybersecurity Framework in Relation to NIST, COBIT and DHS Frameworks." *AIAA AVIATION 2020 FORUM*, pp. 2930, 2020.
- [69] B. Kotkova. "Information Systems and Technologies for the Safe Operation of Airports." *Proceedings of the 26th International Conference on Circuits, Systems, Communications and Computers*, IEEE, pp. 161-166, 2022.
- [70] R. A. Ramadan, B. W. Aboshosha, J. S. Alshudukhi, A. J. Alzahrani, A. El-Sayed, and M. M. Dessouky. "Cybersecurity and Countermeasures at the Time of Pandemic." *Journal of Advanced Transportation*, Vol. 2021, No. 1, 2021.
- [71] Trend Micro, *The case for making BYOD safe-security news*. Available Online at <https://www.trendmicro.com/vinfo/us/security/news/internet->

- of-things/the-case-for-making-byod-safe, accessed on 1 February 2024.
- [72] C. Brook, *The Ultimate Guide to BYOD Security: Definition & More*. Available Online at <https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>, accessed on 1 June 2023
- [73] A. Bridgwater, *How mobile device management is taking on the BYOD challenge*. Available Online at <https://www.theregister.com/2014/11/08/mobile-working/>, accessed on 1 June 2023.
- [74] Y. Joshi, D. Das, and S. Saha. "Mitigating Man in the Middle Attack Over Secure Sockets Layer." *Proceedings of the 2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, pp. 1-5, 2009.
- [75] M. Marlinspike, *New Tricks for Defeating SSL in Practice*. *Black Hat USA*, Available Online at <https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>, accessed on 1 June 2023.
- [76] Norton, *Public Wi-Fi: An Ultimate Guide on the Risks + How to Stay Safe*. Available Online at <https://us.norton.com/blog/privacy/public-wifi>, accessed on 1 February 2024.
- [77] S. Englehardt, D. Reisman, C. Eubank, et al. "Cookies that Give You Away: The Surveillance Implications of Web Tracking." *Proceedings of the 24th International Conference on World Wide Web*, Florence, Italy, pp. 289-299, 2015.
- [78] X. Zheng, J. Jiang, J. Liang, et al. "Cookies Lack Integrity: Real-World Implications." *Proceedings of the 24th USENIX Security Symposium*, Washington, D.C, pp. 707-721, 2015.
- [79] S. Sivakorn, I. Polakis, and A. D. Keromytis. "The Cracked Cookie Jar: HTTPS Cookie Hijacking and the Exposure of Private Information." *Proceedings of the 2016 IEEE Symposium on Security and Privacy*, pp. 724-742, 2016.
- [80] S. Sivakorn, A. D. Keromytis, and J. Polakis. "That's the Way the Cookie Crumbles: Evaluating HTTPS Enforcing Mechanisms." *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, 2016.
- [81] S. Sivakorn, P. Sirawongphatsara, and N. Rujiratanapat. "Web Encryption Analysis of Internet Banking Websites in Thailand." *Proceedings of the 17th International Joint Conference on Computer Science and Software Engineering*, pp. 139-144, 2020.
- [82] M. Kacic, P. Hanacek, M. Henzl, and P. Jurnecka. "Malware Injection in Wireless Networks." *Proceedings of the 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, Vol. 01, pp. 483-487. 2013.
- [83] A. Zimba, Z. Wang, and M. Mulenga. "Cryptojacking Injection: A Paradigm Shift to Cryptocurrency-based Web-centric Internet Attacks." *Journal of Organizational Computing and Electronic Commerce*, Vol. 29, pp. 40-59, 2019.
- [84] J. Spaulding, A. Krauss, and A. Srinivasan. "Exploring an Open WiFi Detection Vulnerability as a Malware Attack Vector on iOS Devices." *Proceedings of the 7th International Conference on Malicious and Unwanted Software*, pp. 87-93, 2012.
- [85] Krebson Security, *Why is 'Juice Jacking' Suddenly Back in the News?*. Available Online at <https://krebsonsecurity.com/2023/04/why-is-juice-jacking-suddenly-back-in-the-news/>, accessed on 1 February 2024.
- [86] Kaspersky, *What is an Evil Twin Attack? Evil Twin Wi-Fi Explained*. Available Online at <https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks>, accessed on 1 February 2024.
- [87] V. Roth, W. Polak, E. G. Rieffel, and T. Turner. "Simple and Effective Defense Against Evil Twin Access Points." *Wireless Network Security*, pp. 220-235, 2008.
- [88] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, and D. Sicker. "Practical Defenses for Evil Twin

- Attacks in 802.11." *Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1-6, 2010.
- [89] Palo Alto Networks, *What Is Network Segmentation?*. Available Online at <https://shorturl.at/rCIDK>, accessed on 1 June 2023.
- [90] The Local Austria, *Turkish suspect identified in Vienna airport cyberattack*. Available Online at <https://www.thelocal.at/20170228/suspect-identified-in-vienna>, accessed on 1 June 2023
- [91] H. Abbas, N. Emmanuel, M. F. Amjad, et al. "Security Assessment and Evaluation of VPNs: A Comprehensive Survey." *ACM Computing Surveys*, Vol. 55, No. 13s, pp.1-47, 2023.
- [92] CISA, *2021 Top Routinely Exploited Vulnerabilities*. Available Online at <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-117a>, accessed on 1 June 2023.
- [93] TechTarget, *The Mirai IoT Botnet holds strong in 2020*. Available Online at <https://shorturl.at/GMUA8>, accessed on 1 June 2023.
- [94] Keyfactor, *Top 10 IoT Vulnerabilities in Your Devices*. Available Online at <https://www.keyfactor.com/blog/top-10-iot-vulnerabilities>, accessed on 1 June 2023.
- [95] Bloomberg, *China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies*. Available Online at <https://shorturl.at/tMHdW>, accessed on 1 February 2024.
- [96] WIRED, *Hacker Lexicon: What Is a Supply Chain Attack?*. Available Online at <https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/>, accessed on 1 June 2023.
- [97] M. Theoharidou, S. Kokolakis, M. Karyda, and E. A. Kiountouzis. "The insider threat to information systems and the effectiveness of ISO17799." *Computers & Security*, Vol. 24, pp. 472-484, 2005.
- [98] MITRE. *MITRE ATT&ACK Matrix for Enterprise*. Available Online at <https://attack.mitre.org/>, accessed on 1 September 2024.
- [99] SecureList, *DarkVishnya: Banks attacked through direct connection to local network*. Available Online at <https://securelist.com/darkvishnya/89169/>, accessed on 1 February 2024.
- [100] SecureWorks, *Gold Sahara*. Available Online at <https://www.secureworks.com/research/threat-profiles/gold-sahara>, accessed on 1 February 2024.
- [101] Google, *Turla: A Galaxy of Opportunity*. Available Online at <https://cloud.google.com/blog/topics/threat-intelligence/turla-galaxy-opportunity>, accessed on 1 February 2024.
- [102] CANSO, *CANSO Standard of Excellence in Cybersecurity*. Available Online at <https://canso.org/publication/canso-standard-of-excellence-in-cybersecurity/>, accessed on 1 February 2024.
- [103] Airports of Thailand (AOT), *AOT ICT Security Policy, AOT Cyber Security Policy and AOT Personal Data Protection Policy*. Available Online at <https://corporate.airportthai.co.th/th/cybersecurity-th/>, accessed on 1 February 2024.
- [104] TSA, *TSA issues new cybersecurity requirements for airport and aircraft operators*. Available Online at <https://shorturl.at/eXlvZ>, accessed on 1 June 2023.
- [105] T. Szuba. *Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security*. National Center for Education Statistics, 1998.
- [106] ICAO, *Annex 17 - Aviation Security; ICAO - International Standards and Recommended Practices*. Available Online at <https://shorturl.at/JQHkr>, accessed on 1 February 2024.
- [107] ICAO, *AVIATION CYBERSECURITY. (2022)*, Available Online at <https://www.icao.int/aviation-cybersecurity/Pages/default.aspx>, accessed on 1 February 2024.
- [108] S.-J. Lee, H.Y. Shim, Y.R. Lee, T.R. Park, S.H. Park, and I.G. Lee. "Study on Systematic Ransomware Detection Techniques." *Proceedings of the 24th International Conference on Advanced Communication Technology (ICACT)*, pp. 297-301. 2022



- [109] MITRE, *MITRE ATT&CK Matrix - Data Encrypted for Impact*. Available Online at <https://attack.mitre.org/techniques/T1486/>, accessed on 1 February 2024.
- [110] J. Katz. "Universally Composable Multi-party Computation using Tamper-proof Hardware." *Advances in Cryptology – EUROCRYPT 2007*, pp. 115-128, 2007.
- [111] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, and T. Rabin. "Algorithmic Tamper-proof (ATP) Security: Theoretical Foundations for Security Against Hardware Tampering." *Theory of Cryptography Conference TCC 2004*, 2004.
- [112] MITRE, *MITRE ATT&CK Matrix - Network Denial of Service*. Available Online at <https://attack.mitre.org/techniques/T1498/>, accessed on 1 February 2024.
- [113] WIRED, *GitHub Survived the Biggest DDoS Attack Ever Recorded*. Available Online at <https://www.wired.com/story/github-ddos-memcached/>, accessed on 1 February 2024.
- [114] I. A. Shah, N. Jhanjhi, and S. Brohi. "Cybersecurity Issues and Challenges in Civil Aviation Security." *Cybersecurity in the Transportation Industry*, pp. 1-23, 2024.
- [115] D. S. Turetsky, B. H. Nussbaum, and U. Tatar. *Success Stories in Cybersecurity Information Sharing*. The College of Emergency Preparedness, Homeland Security and Cybersecurity University at Albany, 2020.