IRJCS: International Research Journal of Computer Science
Volume 11, Issue 08, August 2024
ISSN: 2393-9842
https://www.irjcs.com/archives

Cyber Security and Artificial Intelligence in Aviation

Sidharth Jain
The Shriram Millennium School, Noida, INDIA
sidhjain913@gmail.com
Arnav Bansal
Heritag eXperiential Learning School, Gurugram, INDIA
arnav4314@ggn.hxls.org
Naresh Kumar Agarwala
Indian Institute of Technology, Kharagpur, INDIA
nares_agarwal@yahoo.com

Publication History
Manuscript Reference No: IRJCS/RS/Vol.11/Issue08/AUCS10081
Research Article | Open Access | Double-Blind Peer-Reviewed
Article ID: IRJCS/RS/Vol.11/Issue07/AUCS10081
Received: 30,July 2024, Revised: 08, August 2024 | Accepted: 20 August 2024 Published Online: 27, August 2024
http://www.irjcs.com/volumes/Vol11/iss-08/02.AUCS10081.pdf
Article Citation: **Sidharth,Arnav,Naresh (2024)**. Cyber Security and Artificial Intelligence in Aviation. IRJCS: International Research Journal of Computer Science, Volume 11, Issue 07 of 2024 pages 551-558
doi:> https://doi.org/10.26562/irjcs.2024.v1108.02
BibTeX **Sidharth**@2024Cyber

Copyright: ©2024 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract: Airports are becoming increasingly interconnected and technologically advanced ecosystems. Airports handle sensitive data and depend on interconnected systems, which, while improving efficiency, also heighten vulnerability to cyber threats like data breaches and ransom ware. Additionally, with technological advancements artificial intelligence also plays a huge role, providing a new definition to cyber security in aviation. This paper examines the current state of cyber security in the aviation industry, implementation of artificial intelligence and how we can make the best use of technology, whilst focusing on the vulnerabilities and threats that accompany the adoption of advanced technologies such as Internet of Things (IoT) and Supervisory Control and Data Acquisition (SCADA) systems. The paper also explores the types of cyber attacks that can target smart airport systems, emphasising the need for robust cyber security measures to protect these critical infrastructures.

Keywords: cyber-security; internet of things; smart airports, artificial intelligence, supervisory control and data acquisition;

I. INTRODUCTION

With the rise of new technologies and increase in growth of Aviation industry, airports have adapted new operation and business models. By 2029, the Aviation Market size is expected to be reaching USD 396.15 billion, growing at a CAGR of 2.87% (mordor intelligence). To keep up with this demand airports have incorporated technologies like Internet of Things (IoT) and Supervisory Control and Data Acquisition (SCADA), opening the industry to a whole new air transportation ecosystem and with it new cyber threats. The aviation industry is an important factor is a countries GDP and development, making its security an important concern. According to the International Air Transport Association (IATA), the aviation industry supports over 65million jobs worldwide and contributes approximately $2.7 trillion to global GDP. Beyond its economic impact, aviation also supports essential services such as medical transportation and disaster relief, enhancing public welfare and safety. Artificial duty shared by airlines, airport operators, technology suppliers, and regulatory agencies is safeguarding airports against cyber crimes. Airports handle sensitive data and depend on interconnected systems, which, while improving efficiency, also heighten vulnerability to cyber threats like data breaches and ransom ware. Regulatory frameworks, including the U.S. Homel and Security Presidential Directive and the European NIS directive, mandate stringent protections for critical infrastructure. Prioritizing cyber security in the aviation industry ensures the safety and smoothness of global air travel. This work examines the current state of cyber security and artificial intelligence in the aviation industry, focusing on the vulnerabilities and threats that accompany the adoption of advanced technologies such as IoT, SCADA and AI systems. It also explores the types of cyber attacks that can target smart airport systems, emphasizing the need for robust cyber security measures to protect these critical infrastructures. The rest of this paper is structured as follows: Section 2 discusses airport classification based on technological adoption. Common Vulnerabilities are reviewed in Airports in section 3. Section 4 discusses Cyber attacks that exploit the vulnerabilities. While in section 5 explores the implementation of artificial intelligence in the aviation industry. Section 6 is centred around the market leaders' outlook on artificial intelligence. The integration of cyber security and artificial intelligence is discussed in section 7. Section 8 dives into practices that improve cyber security and eradicate risks. Finally, section 9 concludes the research work.

II. Characterization of Airports Based on Technology

With the introduction of new operational and monitor systems, airports have evolved to make processes automated and thus efficient.

Airports can be categorized into three progressive stages: basic, agile, and smart, each representing different levels of technological adoption. Basic airports focus on the primary functions of managing aircraft operations and providing essential passenger services. They have been automated the least and do not have technology interconnecting different systems. Usually in this model, the airport provides real estate and infrastructure while airlines and other tenants manage their own business. Agile airports employ a centralized service's strategy, offering shared technological services like managed communications and broadband, which leverage basic common use technologies like broadband and Wi-Fi to increases the collaboration between the businesses. Smart airports utilize one single network that enables high speed data flow between all systems of the airport, airlines and 3rd party vendors. These networks involve internet of things (IOT) technology that enables data flow between devices and cloud, as well as Supervisory Control and Data Acquisition (SCADA) that monitors and controls equipment. This increases airport efficiency and makes customer experience better.

III. Common Vulnerabilities in Airports

Cyber attacks focus on exploiting area soft vulnerability from backend systems; hence in order to understand them it is important to examine the vulnerabilities present in airports. In providing a holistic solution to cyber threats we must consider the drawbacks of new technologies adopted by smart airports and outdated flawed technologies used by agile / basic airports.

Major vulnerabilities present in airlines/airports have been highlighted below.

A. Vulnerabilities in SCADA and IoT

With the application of operational technology systems such as Supervisory Control and Data Acquisition (SCADA) system, and Internet of Things (IoT) in the aviation industry; airport processes such as baggage claim, ticketing, etc. have become interconnected. This results in data flows between multiple interconnected systems, devices and sensors, thus opening several points of connection leading to a larger attack surface. Hence, there are more opportunities for cybercriminals to exploit weaknesses. DC Researchers estimate that 10 per cent of attacks will target IoT and advise airports to secure their OT connected systems and networks. Airports utilize SCADA-type industrial control systems for operations like building management, HVAC, utilities, and luggage systems etc. Although SCADA networks are disconnected from the Internet, they are still vulnerable. A key reason for this is many airports use outdated SCADA systems that lack cryptographic protocols thus the data being transmitted is not encrypted or has basic protection. This allows for commands sent to and from a SCADA device to easily be intercepted, altered, or forged by an attacker. Thus, if unauthorized access to the software is gained (through phishing, human error, etc.) data is easily accessible. An example of this is the cyber attack on a Ukrainian power plant's SCADA systems, in 2015, by using phishing emails to install a malware and destroy data. Additionally, it is important to note that just VPNs are not sufficient security and can be bypassed with physical access to the systems. Access to the Remote Terminal Units or insecure communication channels would allow for hackers to make unauthorized changes.

B. Vulnerabilities in ADS-B

In modern airports traditional sonars have been replaced with Automatic Dependent Surveillance-Broadcast (ADS-B) technology. This surveillance technique allows aeroplanes to automatically send and received at a such as identity, position, and identity, information, etc. as needed through a data ink, when they are in a broadcast mode. The problem with ADS-B systems is that they lack inbuilt security measures such as encryption or authentication, to protect the ADS-B data during transmission. This lack of security makes the system vulnerable to various types of attacks such as:

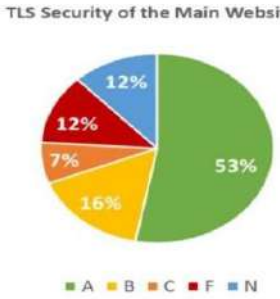
- Message injection: ADS-B technology does not have an authentication system, hence it cannot verify if a message is from a legitimate source. Thus, attackers can use existing technology to mimic actual ADS-B messages and release them in the communication channels.
- Message deletion: By ADS-B generating a signal synchronized with the target ADS-B signal but in opposite phase the attacker can cancel out the target ADS-B signal, destroying the message. This can cause the aircraft to disappear from surveillance and increase the risk of collision as pilots rely on messages to navigate. Additionally, ADS-B systems can correct up to only 5-bit errors, if a message exceeds this limit it gets deleted.
- Message Modification: The attacker transmits a high-power signal to alter a legitimate message or superimposes fake information onto the legitimate message, changing the message. This allows the hacker to hijack the aircraft remotely.
- Eavesdropping: ADS-B transmits data in plaintext, over communication channels, allowing any third party with a radio frequency transceiver to receive its information. This information can be used by terrorist organizations to intercept flights. Some countries, like the UK have passed laws that limit the ability of unauthorized parties to intercept broadcast data.
- Jamming: ADS-B technology doesn't have the ability to detect and resolve collisions between simultaneous data transmissions. Thus, by sending a large amount of data on the same frequency used by ADS-B, an attacker can bring the broadcasting system to a halt.

C. Vulnerability in Web Applications

Most airport/airline websites hold data includes:

- Passenger information such as frequent flyers, names, contact details, passport numbers, and travel itineraries.
- Payment information of transactions for services
- Employee data
- Operational data

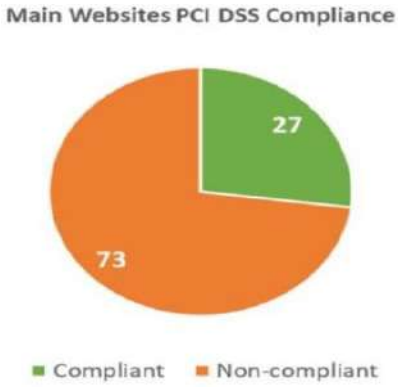
This information if leaked can lead to phishing attacks, identity theft, etc. Thus, it's shocking to see that most airlines don't use cryptographic security on their websites. In a report done by Immuni Web on the world's Top 100 Airports (2019), selected by Skytrax, it was found that 12% of websites still used SSLv3 (Secure Sockets Layer version 3) encryption and 12% had no encryption at all. SSLv3 was created in 1996 and is now considered obsolete due to several security issues. In 2014 POODLE (Padding Oracle On Downgraded Legacy Encryption) attack was disclosed that exploits the way SSLv3 handles padding in block cipher modes, allowing attackers to decrypt encrypted data. The report also states 47% of websites do not have sufficient encryption as most airports do not use protocols such as Transport Layer Security (TLS) have enhanced security features, stronger encryption algorithms, and are equipped to deal with modern cyber threats.



Grade	Quantity	Description
A+	15	No single issue or misconfiguration found
A	38	Minuscule issues found or slightly insufficient encryption hardening
B	16	Several minor issues or insufficient encryption hardening
C	7	Security vulnerabilities or several serious misconfigurations found
F	12	SSLv3 or an exploitable security vulnerability found
N	12	No encryption

Source: ©2024ImmuniWeb

The findings also showcase that 73% of airline websites fail to meet PCI DSS (Payment Card Industry Data Security Standard) standards, designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.



Source: ©2024ImmuniWe

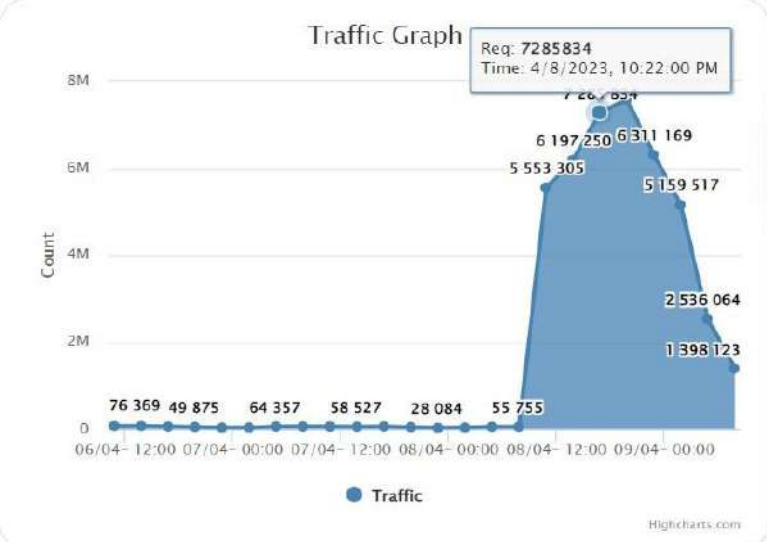
IV. Exploration of Vulnerabilities – Common Cyber Attacks in aviation

The adoption of Industrial Internet of Things (IoT) devices and smart applications has transformed airports into sophisticated, interconnected ecosystems. This evolution, while significantly beneficial, has also introduced new cyber security challenges. This section explores the potential cybercrimes that can target smart airport systems, highlighting the importance of robust cyber security measures to protect these critical infrastructures.

A. DDoS attack

A central feature of smart airports is the interconnection between several different systems/processes, with the integration of communication channels allowing for data flow, done through control and monitor systems like IoT and SCADA. In a Distributed Denial of Service (DDoS) the hacker installs malware into multiple internet-connected devices with poor security which allows them to control the devices remotely. These compromised devices are known as a botnet. The botnet then sends a massive number of simultaneous requests to the server's i.e a website, IoT / SCADA networks, etc. This consumes and overwhelms the server capacity that makes it unable to respond to legitimate requests.

The attacker can demand a ransom in exchange for halting the DDoS attack, although it's more common for DDoS attacks to serve as a deception for the security team, while the hackers steal passwords, credit card numbers, or identity information. During the attack during the attack internet-connected resources like cloud services, passenger-airline communication systems, and common communication networks are vulnerable. One such attack recently took place on April 8, 2023 when a group named 'Anonymous Sudan' launched a significant cyber attack on 6 major Indian airports that involved around 5 million sustained requests. The attack combined layer 3-4 DDoS attacks, which target the network and transport layers to over whelm the infrastructure, with Layer 7DDoS attacks, which flood application services with requests to exhaust server resources. This multifaceted assault disrupted website operations for 9 hours. The graph below shows the spike in an airport website during the attack.



Source: Economic Times

B. Attack on Network

A new system being incorporated in Smart airports allows employees to use their personal devices for work purposes, enhancing convenience and flexibility; this is known as Bring Your Own Devices (BYOD). This allows airport employees to use their enterprise login credentials to connect their personal devices to the airport's secure network. This access does not require permission from an administrator. Thus, by using phishing emails hackers install malware in employee's devices attackers can gain access to standard and restricted internal networks to exchange information. If a BYOD device is compromised, it can serve as an entry point for attackers to infiltrate airport systems. A study conducted by Gartner Mobile and Airtight Networks on 14 major airports in US, Canada, and Asia, found that 80% of the airport network are using outdated encryption and 10% of the laptops had malware (Info security, 2008).

C. Attack on self-service stations

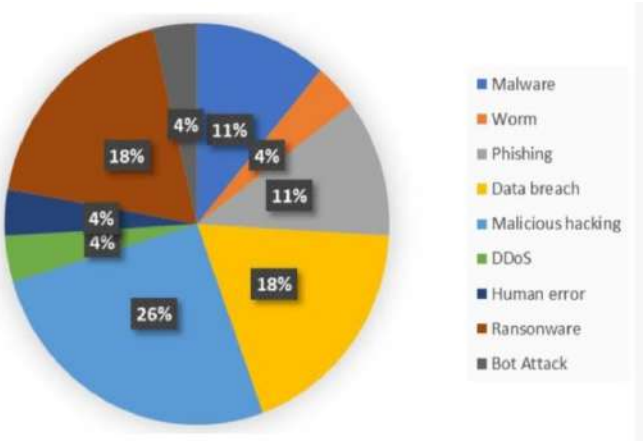
Airline companies utilize the Common Use Passenger Processing System (CUPPS) to provide fast customer support, efficient check-ins and allow multiple airlines to share the same check-in and boarding equipment at airports. This includes self-service kiosks, automated bag drops, and biometric scanners. The majority of these devices operate on commonly used operating systems, firmware, or proprietary software and are connected to the intranet to access company servers, and could be victim to tampering as they are in exposed/public locations. If the attacker gains unauthorized access to these machines, it can be used to change the data stored by the machine and becomes a gateway to getting access to other systems like speakers and monitors.

d) Attack on CCTV Camera:

Airports CCTV systems are now interconnected with other airport information systems thus If the network security is weak, attackers can gain unauthorized access and monitor the airport. Additionally, during security updates the hacker can install malware and temporarily shut down CCTV cameras.

e) Phishing Attacks:

Attackers send airport employees emails that impersonate official mails and contain malicious links. These, if clicked can install malware, or lead to duplicates of official websites where employees are asked to enter data. Additionally, Attackers can also create a fake Wi-Fi networks that that capture credentials and personal information when users login. Further, 3D phishing, creates near identical websites, making these email harder to detect. In 2022, Between July 3-7,over 1700 employees of American Airlines fell victim to a phishing emails sent by other employees, leading to hackers accessing the airline's Microsoft 365 environment and employee's email inboxes. The hacker exploited the IMAP protocol and gained access to employee user names and passwords, as IMAP does not have encryption. They used the compromised credentials to send out additional phishing emails, often masquerading as legitimate internal communications. Office 365 servers also do not have inbuilt encryption on servers. A study on Cyber-Attacks in Aviation Industry (2001–2021), reported 70% focused on the theft of log in details such as administrative passwords and malicious hacking to gain unauthorized access (Elochukwu Ukwanduet al).



Source: Elochukwu Ukwanduet al

Phishing was seen as the 3rd most frequent cyber attack.

f)Worm:

In a worm attack, a self-replicating malicious software program spreads rapidly across computers and networks without requiring any user interaction. It can cause significant damage by consuming band width, overloading servers, and carrying other viruses like spyware. On May 3rd, 2004 a worm attack caused disruption in checking and baggage systems and prevented employees from checking their email.

Ransom ware: In ransom ware attack malicious software, infiltrates a computer system and encrypts the victim's data and rendering it in accessible till the ransom is paid. On 25th of December 2019, an Albany airport face da ransom ware attack when a crypto virus entered the Airport's system and encrypted backups files and administrative files like Excel documents holding budget data. The airport exceeded its insurance deductible and had to pay an additional 25,000 to get the data back.

g) Attacks on Payment Systems:

Attacker can steal sensitive financial information, such as credit card numbers, bank account details, and payment credentials, from airport servers. In 2017, a cyber attack stole over 380,000 payment details, between 21st of August and 5th September of everyone that made a transaction on the British Airways website/mobile app.

V. Inclusion of Artificial Intelligence in Aviation

Artificial Intelligence is playing a crucial role in every single aspect of our current digital world, and the field of aviation is no exception. It is important to shed light upon the fact that most people have no idea how artificial intelligence is being implemented outside the world of generative chatbots. Aviation has a huge scope to further include artificial intelligence within various facets, allowing the society, businesses and the government to reap the benefits. This section will further explore the current applications of artificially intelligent systems in the field of aviation.

a) Flight Management Systems:

Through the integration of artificial intelligence into flight management systems internal and external tasks of an airplane can be conducted automatically, quite seamlessly. Menial internal tasks as in monitoring and maintaining the machinery, eradicating the need to take engineers and mechanics on board. Furthermore, external tasks: flight route and navigation can be specifically curated for a particular flight, depending on the weather conditions, air trajectories and numerous other factors. An artificially intelligent FMS has been used by the German aviation company Lufthansa, helping them predict wind patterns and formatting specific flight routes according to the prediction. This is not only beneficial interns of monetary value but also from an environmental point of view, reducing the fuel consumption and hence reducing pollution propagating sustainability.

b) Customer Assistant

Not only is artificial being incorporating into the backend of the aviation sector, but it is being actively used to enhance the customer experience. There are various functionalities brought to customers with the help of artificial intelligence, some include: personalized check in, quicker baggage drops, curated experiences of in-flight entertainment, and various others. Heathrow has recently partnered with Capgemini, to provide customers with an artificial intelligent assistant. The software being used to achieve this is Sales force's Einstein AI, bringing a whole array of new functionalities for the consumers.

c) Baggage Scanning System

Through artificially intelligents of tware and systems, the aviation field can drastically reduce crimes like trafficking, by scanning the luggage of users. This would remove the doubt of human error and corruption via the airport security as an automated system could conduct the same activities – with greater efficiency and reliability. Heathrow has teamed up with Smiths Detection to create an artificial intelligent model which can detect wildlife trafficking. Till now they've achieved a 70% success rate, with the model being able to go through 250,000 bags per day.

d) Automated Maintenance Systems

Via artificial intelligence maintenance systems can be trained and automated, decreasing the time and effort required to maintain flights. "Predix", General Electric's AI system is aimed at achieving this goal, significantly boosting maintenance and diagnostic capabilities.

Through the high volume of engine and aircraft data by which this model has been trained through, analysts are easily able to forecast faults and plan repairs beforehand – decreasing the risks of aircraft failure.

VI. Artificial Intelligence and Cyber security

Through immediate resolution due to automation, artificial intelligence can exponentially reduce the time it takes cyber security systems to respond to such attacks. This could be understood using a real world case study of the Crowd Strike outage, which was a result of a failure in the software update of the falcon system. If there was an artificial intelligence verification system in place, the outages faced throughout the world wouldn't have existed due to instant identification and resolution of the same. It is extremely important to understand the fact that such artificially intelligent cyber security systems should ensure that all software from the backend to the frontend should be secured and monitored, due to the already stated fact of interconnectedness of systems in the aviation industry. The use of intelligence (AI) systems although revolutionary faces the risk of being manipulated in ways that could compromise their efficiency and security. Attacks, like input attacks, adversarial attacks, model inversion attacks, membership inference attacks, evasion attacks, model stealing attacks and backdoor attacks all exploit vulnerabilities, in AI systems to manipulate them for purposes. These manipulations can distort the AIs learning process influence its decision making capabilities expose information and even trigger behaviors tricking people into sharing information can impact how AI functions, known as engineering. Overfitting attacks take advantage of AI models excelling with data but failing with data. Model drift occurs when data changes over time affecting the accuracy of AI systems. These tactics highlight the importance of defences regular monitoring and updates to keep AI secure and dependable. Input attacks, which is an attack which is done by feeding certain training data into artificial intelligence systems, allowing the output to be manipulated; Poisoning attacks are attacks which corrupt the artificial intelligent software resulting in system malfunctions according to the desires of the threat actor . The only way through which security against such sophisticated attacks can be achieved are constant artificial intelligence sustainability tests, updates in data policies and attack response implementations.

VII. Suggestions to Navigate and Combat Cybercrime

It is important for airlines and airports to continuously strengthen their cyber security measures. Effective cyber security protects sensitive data and ensures efficiency of operations. To safeguard against potential breaches and attacks, it's important to be proactive and consider a holistic approach to cyber security. This section details specific practices and suggestions for airlines to ensure digital hygiene.

a) Procedures that should be conducted regularly to ensure if a breach occurs it is detected instantly, and vulnerabilities do not go unnoticed:

I. Monitoring and conducting updates on software and hardware: Staying up to date with versions of applications is an essential part to fixing vulnerabilities.

II. Conducting cyber audits on SCADA/IOT systems, ISMS, incident response capability systems.

III. Monitoring CCTV cameras: Smart airports have begun to utilize AI-powered surveillance systems to analyse footage in real time and flag threats.

IV. Supply Chain Mapping: Monitoring and analysing all entities involved in the supply chain to detect potential vulnerabilities.

V. Running virus detecting and anti-malware software, daily.

b) Airports have existing technology which has become outdated with the emergence of new cyber threats. To ensure their safety it is important to modify the existing applications in order for them to meet the standard of modern cyber security. Suggested modifications:

I. Installation of firewalls and network segmentation on networks and websites: Firewalls form a barrier between an organization's intranet and insecure net and helps filter out dangerous data and code.

II. Applying strong user authentication protocols: To protect sensitive data and even physical servers of SCADA/ IOT systems airports should use a combination of biometric authentication and Multifactor authentication. This will ensure access is only provided after two or more evidences are provided. Additionally, employees should be instructed to change default passwords.

III. Regulation of remote access: Remote access allows users to connect to a network or system from a distant location, often via the internet. This capability should be enabled only whilst required, to limit access points for attackers.

IV. Data encryption: Encrypting data on websites, servers, etc. ensures that even if data is stolen it remains inaccessible by hackers, as it is scrambled instead of plaintext. Encryption can be done keeping both encryption and decryption key same (symmetrical encryption), or keeping both keys different (asymmetrical encryption). A symmetrical encryption is more secure as even if one key is compromised the other key is secure.

V. Ensuring the information security management system (ISMS) supplier is ISO27001 certified: ISO 27001 is an international standard to manage information security. ISO 27001-certified supplier's have a comprehensive information security management system that is equipped to identify, assess, and mitigate cyber attacks. Suppliers can help guide airlines in improving their ISMS to combat emerging cyber threats.

c) Investing in new technologies, can be costly but in the long run helps provide stronger measures to be digitally protected against cybercrimes which could end up costing more money.

I. Spread spectrum technology can be used to counteract jamming and eavesdropping in wireless communications in systems like SCADA. It spreads the signal over a wider bandwidth by multiplying the data signal with a spreading code, making it more resistant to interference and harder to intercept.

II. Additionally, it switches the signal between different frequencies within a specific range, making it difficult for unauthorized parties to jam or eavesdrop on the communication.
III. Intrusion Detection Systems (IDS) are crucial for monitoring both software and hardware devices with in a IoT network to detect and respond to potential security breaches. IDS can be categorized into two main types: network-based IDS (NIDS) and host-based IDS (HIDS). NIDS monitors data flow between communications channels analysing suspicious activity or attack patterns. They can help alert threats such as unauthorized access attempts, malware transmissions, and unusual traffic spikes. On the other hand, HIDS is installed on individual hosts or devices, this could be a servers monitors or any other type of device that stores and produces data. HIDS monitors the activities occurring on the specific host, such as system calls, file system modifications, etc. HIDS helps detect unauthorized access to applications and changes to critical system files.
IV. Micro segmentation is a security practice designed to enhance network security by creating isolated segments within a network. This technique involves dividing the network into numerous smaller, secure zones, thus minimizing the attack surface and making it easier to monitor entry of insecure data. Additionally, this ensures that even if an attacker breaches one segment, they cannot move to other parts of the network.

d) A key area where most airports lack is training employees to combat cyber threats and have good digital hygiene habits. These following practices/ plans will help employees from preventing cyber attacks:

I. Basic security awareness training for all employees that use an information system should cover topics such as password management, recognizing phishing attempts, and safe internet usage, in order to establish a foundational understanding of cyber security principles.
II. Providing specialized information security training should be provided to employees with access to sensitive IT systems. This could include training on handling sensitive data, implementing security protocols, identifying and reporting suspicious activities, and understanding regulatory compliance requirements. Additionally, it should help equip personnel with the skills to respond quickly and appropriately to security breaches, minimizing damage and reducing recovery time and costs. Asking these employees to also sign a confidentiality agreement and agree to procedure will also ensure data isn't leaked.
III. Disaster recovery plans for IT assets: Creating a Disaster recovery plans for IT assets helps in quick restoration of critical IT operations post a cyber attack. These plans should include detailed technical procedure store cover and restore systems to a functional state, such as data backups, system reboots, and network reconfigurations. Employees should be assigned specific tasks/roles.

VIII. CONCLUSION

This study comprehensively outlines the evolution of airport technology, artificial intelligence systems and the corresponding increase in cyber security vulnerabilities. Airports are categorized into basic, agile, and smart types, each with varying levels of technological integration, which introduces different cyber security challenges. The paper highlights the significant vulnerabilities associated with SCADA systems, IoT devices, ADS-B technology, web applications, and other critical infrastructure with in airports. Key vulnerabilities include outdated SCADA systems lacking cryptographic protocols, unsecured ADS-B transmissions susceptible to message injection and deletion, and inadequate encryption on airport websites and payment systems. These vulnerabilities expose airports to a range of cyber attacks, including DDoS attacks, network intrusions, phishing, and ransom ware, which can severely disrupt operations and compromise sensitive data. Additionally, the paper provides various techniques through which artificial intelligence can be integrated into aviation, as well as real world instances for the same. This paper also emphasizes the need for robust cyber security measures. These include the adoption of firewalls, network segmentation, strong user authentication, regular software updates, and comprehensive employee training programs to enhance digital hygiene and cyber security awareness. Furthermore, this research suggests implementing advanced technologies such as spread spectrum communication to counteract jamming and eavesdropping, and intrusion detection systems (IDS) for real-time monitoring and threat detection. The emphasis on proactive measures, such as regular cyber audits, data encryption, and investing in new technologies, is crucial for mitigating cyber threats and enhancing the overall security posture of airports. In conclusion, as airports continue to evolve into highly interconnected and technologically advanced ecosystems, airport staff, government and third-party vendors have a shared duty for safeguarding Smart airports against emerging cyber threats whilst in corporation artificial intelligence to ensure the growth of the industry. Hence, in order to combat cyber threats a collaborative multi-layered security frame work is required. Along with technology advancements, cyber threats and associated dangers will only increase, and in the context of aviation, cyber threats should be taken more seriously now than ever.

REFERENCES

1. Lykou,G.,Anagnostopoulou,A.,&Gritzalis,D.(2018).Smart Airport Cyber security: threat mitigation and cyber resilience controls. Sensors, 19(1), 19. https://doi.org/10.3390/s19010019
2. Ali,T.,Hussain,A.,Khan,S.Z.,Gohar,M.,Rasheed,M.A.,&Rahim,N.(2021).Areview of passenger digital information privacy concerns in smart airports .Journal of Transportation and Security,14(2),127-150. https://doi.org/10.1007/s12198-02100244-1
3. KHAN,L.U.,YAQOOB,I.,TRAN,N.H.,DANG,T.N.,HONG,C.S.,&HONG,P.(2019). EDGE COMPUTING ENABLING SMART CITIES: A comprehensive survey. Sensors,19(1),19. https://doi.org/10.3390/s19010019

4. Cisco Systems, Inc.(2020). Passenger experience in smart airports: A point of view. Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf
5. Lin,J.,Wang,H.,Ma,Y.,&Yang,X.(2020).A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal,7(5), 4163-4195. https://doi.org/10.1109/JIOT.2020.2992024
6. QALtd.(2020).SCADA threats: Research paper. Retrieved from https://www.qa.com/media/13629/scada-threats-researchpaper.pdf
7. Milinković,S.(2013). Big data management in smart cities. International Journal for Traffic andTransport Engineering. 3(4), 322-332. Retrieved from http://ijtte.com/uploads/2013-12-30/5ebd908d-7f47-e96dIJTTE_Vol%203(4)_2.pdf
8. Color Tokens Inc. (2021). Cyber security for airports: Threats and mitigation strategies. Retrieved from https://colortokens.com/blog/cybersecurity-for-airports-threatsmitigation/
9. Gulf News. (2004,May3). Worm wreaks havocon computer networks. Retrieved from https://gulfnews.com/uae/wormwreaks-havoc-on-computer-networks-1.321264
10. Industrial Cyber security Pulse. (2020). Throwback attack: Hack leaves 1400 passengers of Polish airline LOT stranded. Retrieved from https://www.industrialcybersecuritypulse.com/threatsvulnerabilities/throwback-attack-hack-leaves-1400-passengersof-polish-airline-lot-stranded/
11. The Hindu. (2018, September 7). Data breach in British Airways: 380,000 payment details stolen. Retrieved from https://www.thehindu.com/business/Industry/data-breach-inbritish-airways-380000-payment-detailsstolen/article24890282.ece
12. SCADA International.(n.d.). What is SCADA? Retrieved from https://scada-international.com/what-is-scada/
13. ImmuniWeb.(2020).State of cyber security at the world's top100 airports. Retrieved from https://www.immuniweb.com/blog/state-of-cybersecurity-top100-airports.html
14. Pajic,M.,Pajic,S., & Prasad, N.R.(2020). Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey. IEEE Communications Surveys & Tutorials, 22(4), 2586-2620. https://doi.org/10.1109/COMST.2020.3007589
15. Fortune.(2016,October22). DDoS attack: How hackers profit. Retrieved from https://fortune.com/2016/10/22/ddos-attackhacker-profit/
16. Vitale,Cat. " Heath row Airport Extends Partnership with Capgemini." Airport Technology,17Nov.2023, www.airport-technology.com/news/heathrow-airport-extends-partnership-with-capgemini/.
17. "Ai Revolution in Aviation: Shaping the Future of Air Travel." Symphony Solutions, 8 July 2024
18. "Artificial Intelligence."Airbus,2 July2021,www.airbus.com/en/innovation/digital-transformation/artificial-intelligence.
19. "Digital Acceleration."Digital Acceleration, www.boeing.com/defense/jadc2/digital-acceleration#digital
20. Walch, Kathleen." What Role Does AI Play in Enhancing Aviation Cyber security?" Forbes, Forbes Magazine, 31 July2023,www.forbes.com/sites/cognitiveworld/2023/07/29/what-role-does-ai-play-in-enhancing-aviation-cybersecurity/#:~:text=AI%2Ddriven%20systems%20can%20analyze,the%20risk%20of%20human%20error.
21. "Crowd strike Posts Preliminary Post-Incident Report on Recent Global It Outage: AHA News."American Hospital Association |AHA News, www.aha.org/news/headline/2024-07-25-crowdstrike-posts-preliminary-post-incident-report-recent-global-it-outage#:~:text=The%20outage%2C%20which%20was%20caused,health%20systems%20across%20the%20country.
22. Marcus Comiteretal." Attacking Artificial Intelligence: AI's Security Vulnerability and What Policy makers Can Do about It." Belfer Center for Science and International Affairs, www.belfercenter.org/publication/AttackingAI