Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)

Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry

Shazah Ishtiaq[1] and Nor Azlina Abd Rahman[2,*]

[1,2]*Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia*
[*]*Corresponding author. Email: nor_azlina@apu.edu.my*

ABSTRACT
'Aviation' is referring to transportation of goods via air. The global community is increasing, and people are moving from one place to another in a faster way due to the presence of aviation. As the technology is growing there have been an increase in the cybercrimes as well. The most famous case in the aviation industry is the flight MH370, which was a Malaysian airline travelling normally without any turbulence, disappeared without a trace. The aircraft had 227 passengers boarded including the crew, it is still a mystery which no one could solve. There have been conspiracies that stated that the plane's auto pilot was hacked. Considering the importance of this case, this research will be focusing on the cybersecurity threats which exists in the aviation industry, it will also present threats which may have caused the disappearance and highlight a plan to overcome vulnerabilities in the critical infrastructure of aviation industry.

Keywords: *Aviation industry, air transport, air safety, computer crime, cybersecurity.*

1. INTRODUCTION

Aviation is one of the most important phenomena for global industries, it helps connecting different people, businesses, and cultures across the globe. In this industry, the stakeholders, and the partners play an important role, their role is to work together and increase the benefits of air transport to the fullest. They should support growth of aviation by uniting people and places more. The growth in the aviation has been seen throughout the years, it has also shown a long-term resilience and became the essential means of transport. Historically speaking, the air transport has doubled every fifteen (15) year and it is one of the fastest growing industries as compared to others [1]. In 2016, the weight which was carried worldwide was estimated around 3.8 billion passengers and the revenue passenger kilometres (RPKs) was calculated at 7.1 trillion. Due to the pandemic, all airlines carry carried 1.8 billion passengers which generated the global revenue of 328 billion dollars in 2020 [2]. There has been new development of technologies for more safe services, internet is also amongst these technologies. Nowadays everything is working on the internet, whether it is the infrastructure, or any other service [29-34]. Internet is not a safe place, as it is the easiest path for hackers to breach into companies and steal personal information of the target or try to disrupt the business [35-38]. Further classification of aviation industry is in four categories which are as follows:

- One organization: The International Civil Aviation Organization (ICAO) is a part which the United Nations handles. This organization helps designing the rules which are standards that needs to be followed.
- Governments: There are services like BEA (Bureau d'Enquetes et analyses) and the NTSB (National Transportation Safety Board) which provides security and safety standards within the aviation industry.
- Trading: The trade system in this industry follows the guidelines of International Air Transport Association (IATA) mostly all of the airlines practice its guideline.
- Aircraft's manufacturers: Large companies such as Dassault, Honeywell, Boeing etc., keeps their systems updated from any new emerging threats.

Due to the use of technology in the aviation industry there have been bigger challenges, such as dealing with hackers mainly the cyber-terrorists, this is due to the weight of economy which is more as compared to other industries. This industry is popular for having the safest type of transportation, many threat actors aim more to exploit its vulnerabilities because it is prone to attacks, the reason is because there is less security in this industry.

1.1 Cyber Risks in aviation

Due to its complexity and high weightage in the economy, there have been several attacks which have occurred, the first attack which was experienced was back in 1997, in which a teenager exploited a vulnerability in the telecommunication service of the airport, and he managed to attack it with denial-of-service attack, which concluded that the infrastructure of the telecommunication is weak. There have been remote hacking attacks as well, these attacks mostly target the air traffic control system, the aeroplane, and the airports. Due to these attacks the risks increase in the passport control, the passengers, and the systems that controls the baggage [3]. A consultant called Phil Kernick from CQR consulting stated that there have been attacks occurring on Australian airports on the daily basis. It was reported by the European Aviation agency that the average cyber-attacks that occur monthly in airports are around 1,000 [4]. In 2014, a Tunisian hacker was abler to hack into the computer and communication systems of the US airport. Back in 2015, there was a DDoS attack on Poland's LOT carrier in their flight operation system in its airport. Because of this attack there were about 22 cancellation of flights and it also resulted in leaving around 1,400 passengers deserted [5]. According to Avlaw Aviation, one of the most common attack that occur in the aviation industry are the distributed denial of service (DDOS) attack, this attack helps the threat actor to disable the system and gain access of it. The infrastructure of aviation industry includes airports, air bus, and air transportation etc. According to the research above, it can be presumed that the critical infrastructure of aviation industry is the air transportation.

2. AIR TRANSPORTATION TECHNOLOGY

The growth of the technology has been rapid throughout the years, there have been different systems which are involved for the transportation to work properly and accurately. the Hackers are people who find new ways to try to exploit a system's vulnerability. Following are some of the systems which are used in the air transportation:

2.1 Data Communication

The Federal Aviation Administration (FAA) created a system in which the pilots and air traffic controllers can communicate easily, it is a system with digital text-based communication it is called Data Communication. This system is embedded with pre-written messages which replaces the verbal communication of the pilot. This is better than the verbal communication because it lessens the overcrowding of the frequency and gives a written document of the communications between the controller and the pilot [6]. According to a report by Alan Pellegrini, who is the CEO of the Thales USA stated that there have been numerous hacks in the systems, and data communication was amongst them [7]. As far the information goes there have been no serious records of hacks in this system.

2.2 Wi-Fi

Wi-Fi is a wireless network protocol which is used to connect local devices in a network and also access the internet. But in airplanes, the Wi-Fi is a connection to an access point which has the ability to connect to a network [8]. There are two different types of connectivity which are used in aviation nowadays,

i. Air-to-ground (ATG)
ii. Satellite

There have been no major attacks that have occurred through the Wi-Fi system, but back in 2013, a security officer was able to gain access of the navigation system, and he was able to get into the air traffic control with just the use of his smartphone [9].

2.3 Entertainment

It is widely known as In-flight entertainment, almost all the airlines have this system installed for making a flight more exciting. These systems are connected with a wiring which is inserted in the aircraft walls, this is placed just next to the AC's and the oxygen masks, but a new IFE does not require wirings [10]. The fibre optic is carrying all the data and power. The listening of the music was achieved by a frequency which is called the Automatic Direction Finder (ADF) and then it broadcasts it to the aircraft Public Address (PA) [11]. In 2015, a security expert hacked into the aircraft's in-flight entertainment system and using its vulnerability he slightly made the aircraft fly sideways by changing the commands into the climb mode. According to him he had hacked couple of planes 15 to 20 times. He could achieve this attack by connecting his laptop directly to the IFE and then he was able to hack into the Thrust Management Computer, which had default passwords and ID's [12].

2.4 Air Traffic Control

Air Traffic Control is a very important system which is required in recent aircraft travel. It helps in monitoring the air traffic in a specific area, it uses it skills and intelligence to direct all the flights safely to their destinations. The following area comes under this system such as the tower control, departure and arrival control, and the control of the route [13]. These activities are conducted by the people who are working on the ground. This system has been most vulnerable as compared to other systems, due to which many hackers were able to access various systems in the civil aviation. Back in 2011, hackers gained access to the radio frequencies which was used by the British air traffic controller and gave false information to the pilot [14]. These kinds of attacks can cause serious damages such as the crashing of the plane.

2.5 Satellite Navigation (GPS)

It is a fastest growing type of navigation system in the aviation industry it is called the Global positioning system navigation (GPS). This navigation uses a NAVSTAR satellites which orbits the earth [15]. There are three parts of GPS:

I. One segment is the space.
II. Another one is the control.
III. Lastly, the user

Some hackers also exploit its vulnerabilities as well. A black hat hacker known as Santa Marta, demonstrated an attack on the SATCOM (satellite communications). In this attack he was on the ground and was able to interrupt a non-safety communication which was the Wi-Fi [16].

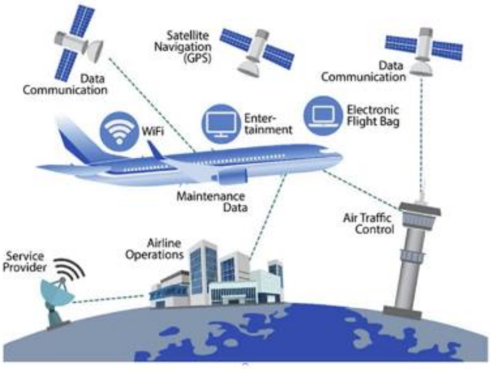


Figure 1 Virtualization of Interlinked systems in civil aviation

3. VULNERABILITIES

To attack the systems of the civil aviation is not that hard, because many attackers have managed to get into the system quiet easily, following are the prominent vulnerabilities which are present in the air transportation systems:

3.1. Voice (Very High Frequency – VHF)

It is called a voice communication which is a main way of the communication between the Air Traffic Control and the airplane. It is used to broadcast all the Air Traffic Control instructions to the airplane, which is then known by the pilots, these reports and requests are also reported to Air Traffic Control by the pilots. The information which gets broadcasted includes, the weather, information about the flight, broadcasts of information related to the airport. This communication is occurring due to the analogue radio, this radio is called VHF (Very High Frequency) and HF (High Frequency). As this service uses a frequency for the communication to work between the aircraft and the ATC, there are high chances of denial-of-service attacks. Many experts stated that the attackers are either using pirate radio stations or buying an aviation transceiver without the license to attack the aircrafts. There have been recorded incidents of spoofing in the voice communication, which is why the need to secure these systems is highly recommended [17]. The intruders who are detected in the VHF are between 30% and 40%, which is why attacks such as jamming can also occur which can effectively disable a VHF this can result in the airplane making use of an unauthenticated data link, which is easier to hack into.

3.2. Automatic Dependent Surveillance-Broadcast (ADS-B)

It is a system in which the airplane broadcasts its own ID, velocity, and position or any other related information such as any urgent codes. These broadcasts occur twice in a second for both the information about the velocity and the position, but the identification of the aircraft occurs on every five seconds. This is an important use in both the European and US airspaces, because this helps in the accuracy of the location [18]. This system is easily exploitable because the messages which are sent are neither using encryption nor it is authenticating it. In a Black Hat USA conference, a researcher named Andrei Costin demonstrated an attack on ADS-B. This attack consisted of a software-defined radio which was bought at a price of $ 1,000, he used an ADS-B receiver so he can spoof the messages that were being accepted by the other receiver. This demonstration showed that attackers can easily intercept these messages and also spoof it [19]. For example, the attackers can install a replay attack in which they can seize the packets of the flight information and can replay them to the system they are targeting.

3.3. Satellite Navigation (GPS)

There has been the recent introduction of NextGen system, in which the heavily use of GPS system will be embedded. There have been many vulnerabilities that can be exploited in the GPS system. A study conducted on the GPS vulnerability stated that, the GPS is vulnerable because of the weak signals which are on the single civilian frequency. Plus, it is very easy to buy a GPS or build one device which can disrupt any other GPS. Attacks such as jamming, could lead to GPS not receiving any signal which can result in an undesirable performance. Spoofing can also deceive pilots and the control systems which can lead to disastrous situations [20]. There are severe attacks such as radio frequency attacks which can cause damage to the electronics and the individuals. Satellite communication uses radio frequency to transfer energy which is why it is prone to all kinds of attacks. According to Santa Marta a cybersecurity researcher, theorized that physical damages can be caused to this system if the attacker applies energy to any part of the aircraft [21].

4. IMPACT OF DDOS ON AIR TRANSPORTATION

There have been a lot of attacks which were mentioned above, it was also discovered that the vulnerabilities in aviation industry are a lot, which gives the attackers privilege to attack on the biggest growing industry easily. It was uncovered earlier in the research that the most attacks that occur in the aircrafts or systems surrounding it are the Distributed denial of Service attack (DDOS). This attack mainly attacks services such as websites or anything which is available online. The main purpose of this attack is to overwhelm the target with so much traffic that is disrupts or slows down [22]. In some severe cases it can destroy the hardware completely or they can encrypt the data and ask for ransom, there are many ways to wrongfully use an information. Table 1 shows the impacts that can occur if there is a possible DDOS attack.

Table 1. Threats and its impact on air transportation

Thread ID	Threats Description	Threat target	Impact
1	Attacking of critical systems via IFE (In-Flight Entertainment Systems)	1. Gain control of the system. 2. lead to the crash of the airplane.	Severe
2	Malware Infection on Wireless Interfaces	It can lead to damage but not that much effort.	Major
3	VHS (Very High Frequency)	1. Can gain control of the information about the airplane. 2. Can broadcast fake information to the pilot or the system. 3. Can result in misdirection of the destination.	Severe
4	Attack on the airplane via Compromised IT	It can damage the network of the airplane.	Major

5. DEFENCE TECHNIQUES

According to the threats and it is impacting the need of defence techniques is very much required in the aviation industry. The impact of an attack causes severe damages to the system and to the infrastructure as well.

5.1. General Security

This paper will focus on evaluating and identifying the information security risks which can be caused by humans, this will be centred on ISO27001. ISO27001 covers all the aspects of management security risk and helps in maintaining the CIA (confidentiality, integrity, and availability) of all the information systems. The minimum standard of security risk is to have a consistent, cohesive, analysable, functional, and cost-effective sensible approach. The security risk management should have the following functions:

i. Security policies
ii. Standard and mindfulness strategies
iii. Security risks
iv. Technical risks

`In the light of information security, this paper will classify the risks of civil aviation as subject threat, management threat, technical threat and legal threat which will be based on the ISO27001 standards. The Figure 2 will show the systematic risk classification.

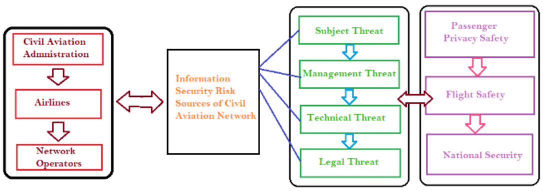


Figure 2 Information Security sources of risks in civil aviation.

5.1.1 Subject Security

The agencies which manage the organization are very important, there should be a creation of information security system in the civil aviation network. If the management is not perfect it can result in the restriction of proper regulations and it can also cause major security disasters. To lessen the damage, the first action is to have an effective supervision organization. The second problem which occurs is the coordination between different managements within the organizations which includes the airlines, the technology, and the government companies. Which can be the reasons why their administration is weak and can be prone to attacks easily.

The most common weaknesses which is found in almost all the industries is the security awareness. The technology is increasing rapidly, and there are attacks such as phishing which targets employees, if employees of the companies are not aware of the dangers of such attacks, there will be major data breaches [23]. The employees should be fully aware of the smart airports and should be more aware on the technologies which are being used in the airports. It is the duty of the technical maintenance and the management to educate the employees as there are rapid increase of cases in the aviation industry.

5.1.2 Management Security

There should be a construction of a prevention and control system against any security risks, there can be seen many attacks in this industry which means that there is a need of this system. There are airplanes that follow both ISO27001 and NIST standards in their management. These both standards are excellent in their own ways, they provide good pointers when discussing the prevention system [23]. The risk analysis of the security has mostly been done by the aircrafts themselves, the only weakness that can be seen is the management of the third-party companies. As mentioned above there can be a high chance that the management is not coordinated. All the networks are interconnected with each other, for example if the IT department is attacked with DDOS, it will 100 percent effect all the departments which relate to it, as IT plays a large role in the companies. The best prevention control system that fits the aviation industry is the Incident response plan. This procedure is important because when it comes to air transportation many things are at stake, the biggest worry is the human life. So how an incident is responded successfully is very important when it comes to aviation.

5.1.2.1 Incident Response Plan (IR)

It is a very thorough approach which should be taken by the organization to prepare for any kind of cyber-attack, this planning includes the detection, containment and recover from an attack. This planning will be effective on any cyber-attacks that can occur in the organization and can help in protecting the assets as well. The goal of this planning is to make sure the business is running after an attack. There are two famous frameworks which are being practiced by mostly all the organizations: SANS (System Admin, Audit, Network, and Security) and NIST (National Institute of Standards and Technology). Following are the steps which can help in responding to a cyber-attack:

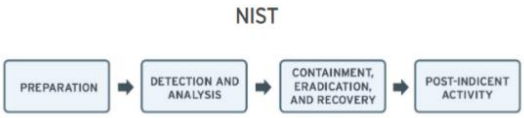


Figure 3 NIST framework

1. *Preparation*

As this framework will be for the critical infrastructure, which is the air transportation, the first phase should be to develop a set of policies and protocols which needs to be followed. The cybersecurity policy means the security and responsibility of an organization. The policies include, password policies, wireless communication policy, remote access policies etc. This can help in being prepared for any time of attacks and help in defending against it. The protocols which should be followed can include, password management, raising awareness, building strong firewalls, and informing people of an attack etc [24].

The second step in this phase, which is very important is to create a response team, this team can help in mitigating attacks when there is an attack. They can help in training and allocating responsibilities to people who can solve cases. The people who were affecting in this attack should also be involved.

2. *Detection, Analysis, and Identification*

As previously mentioned, that the people should know about the incident for example, the response team, government, or officials. If the breach is high for example, the customer's personal data is lost due to the DDOS attack, they should also have knowledge of such attack as per guidelines for protection of data. There should be a follow-up report on each step that was taken during the mitigation, and if the situation is dire use the data protection laws for safety.

The next step that follows, is to detect the attack. In this case is to detect the Distributed Denial of Service Attacks (DDOS). There are many types of DDOS attacks as well, but mostly all attacks are flooding the service with packets and overwhelming it to exhaustion. Following are the ways to detect such kind of attacks:

- The use of detection systems in the Firewall.
- Using anti-virus and anti-spywares.
- Using Intrusion Prevention System and Intrusion Detection Systems
- Hashing the confidential files, so even if there is an attack, it is impact can be minimal.
- There is a popular DDOS detection tool called LOIC (Low Orbit Ion Cannon)

The next part is assessing the impact of the attack, the company need to make sure how many systems were impacted. This can be achieved by

- Using tools to identify any systems that may or may not be affected.
- Get logs from all the systems such as breach detection systems, security events, domain name system (DNS) etc.

3. *Containment, Eradication and Recovery*

The first step in this phase is to isolate the systems which were affected from the network. Isolation of the systems will be done to further investigate them and extract any information which can be found in its volatile memory.

The next step is to eradicate the threat completely from the system and give it for further analysis to security personnel.

- Firstly, remove the risk in the system completely.
- Forward the system to a security vendor to fix and update it.
- This vendor will help in completely cleaning of the system and will scan it by using end point detection.

The last step of this phase will be do start fixing the problems which the attack had done.

- Use tools to analyses the services that were involved in the attack and check for any vulnerabilities.
- Pentest should be done regularly.
- Applying of patches on the systems, also hardening it and cleaning it up completely [25].

4. *Post incident*

After the incident following steps should be taken:

- Recommendations which are provided by the security professionals should be followed. Configure any tools which they recommended.
- Have a depth review in all the layers, so that they are secure.
- All the security policies should be reviewed [25].
- The risk management processes should be reviewed for mitigation of any risks.
- The final report should be shared to the stakeholders.

5.1.3 Technical Security

The most technical risk that can be in the avionics will be technical errors. To fix this problem, the first step should be to mend all the software and hardware technologies in the organization. In the case of DDOS attack, chances are that the hardware might be damaged, to replace it completely is the best way. This change of hardware should do in a well-timed manner to avoid any disruptions in the operating environment. Next, all the technicians who are available should check the operating platforms to detect any vulnerabilities which are present in the system. They should scan the core of the operating systems, database and general softwares [17]. There should monitoring done on these systems 24/7, to avoid any cyber-attacks. Following IT securities will help in defence against DDOS attacks:

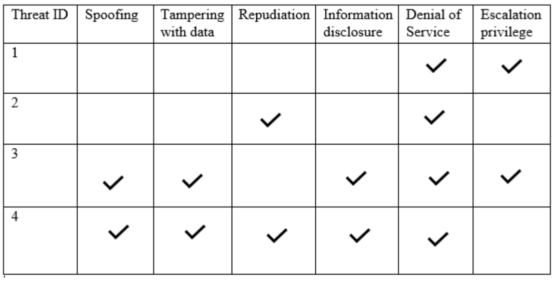
- Application Security
  This security protects from application-level attacks. Best technique is encryption and best tool is web filtering firewall.
- Information Security
  To ensure Confidentiality, Integrity and Availability of data.
- Endpoint Security
  Best practice is to raise awareness.
- Network Security
  To improve the network security include, DLP, Email security, Wireless security, etc. [26]

6. STRIDE MODEL FOR THREAT CLASSIFICATION

STRIDE is a model which was introduced by Microsoft on classifying the types of vulnerabilities that are present in the cybersecurity. This methodology aims to safeguard an application that should meet the demands of Confidentiality, integrity, availability, non-repudiation, authorization, and authentication of the security [27]. The vulnerabilities and can be classified and according to that countermeasures can be produced which can lessen the risk of the attack. STRIDE realizes all the qualities of the vulnerabilities which the attacker uses to exploit. The threat modelling will be concluded on the threats which are mentioned in the Table 2.

- Spoofing: Effect in Authentication
- Tampering: Effect in Integrity
- Repudiation: Effect in Non-Repudiation
- Information disclosure: Effect in Confidentiality
- Denial of Service: Effect in Availability
- Escalation privilege: Effect in Authorization

Table 2. STRIDE threat classification analysis



Threat ID	Spoofing	Tampering with data	Repudiation	Information disclosure	Denial of Service	Escalation privilege
1					✓	✓
2			✓		✓	
3	✓	✓		✓	✓	✓
4	✓	✓	✓	✓	✓	

This analysis can help in characterization of a threat in various situations. This method can show us what the attacker is trying to achieve. According to the case denial of service attack has been marked in mostly all of the threats, this shows us that in aviation the most attack which occurs in the avionics is the Distributed denial of Service Attack [28].

7. CONCLUSION

Aviation is expanding its new technologies daily, the reason for this is because there is a rapid increase in the number of passengers every year. Therefore, every airline tries their best to put new technologies in their companies in order to grow in this industry by giving an enjoyable trip to their customers. Due to the new technologies, there have been risks and threats which are growing with them, this is due to the smart devices which have been used in this industry a lot.

In this paper, proper systems were elaborated which are being used nowadays in the civil aviation. The vulnerabilities which were commonly found in these systems were also mentioned in this work. The critical infrastructure plays a very important role in the industry, if it is somehow affected it can destroy it completely. The critical infrastructure which was highlighted was the air transportation because this main purpose of this industry is to transport people or cargoes etc. By seeing the impact of the most common attack, which was DDOS, it was discovered that severe consequences can be seen. Proper defence techniques were also given for threats and STRIDE which is a threat modelling was applied which showed that the mitigation of risks can happen in cyber security. According to the study, it can be assumed that this industry is attacked very easily and the mystery of the Flight MH370, cannot be a mystery anymore. Because the technology which is used in the industry is high tech, therefore there are high chances that this flight was hacked and made to disappear.

REFERENCES

[1] Uniting aviation, "Aviation benefits: a better future," 2018. https://unitingaviation.com/news/economic-development/aviation-benefits-for-a-better-future/ (accessed Apr. 28, 2021).

[2] E. Mazareanu, "Air transportation - statistics & facts | Statista," 2021. https://www.statista.com/topics/1707/air-transportation/ (accessed Apr. 28, 2021).

[3] J. Haass, R. Sampigethaya, V. Capezzuto, F. Haass, and K. Sampigethaya, "Aviation and Cybersecurity: Opportunities for Applied Research." Accessed: Apr. 30, 2021. [Online]. Available: https://commons.erau.edu/publication.

[4] Avlaw Aviation Consulting, "Cyberattacks in the Aviation Industry - Avlaw Pty Ltd, trading as Avlaw Aviation Consulting," 2020. https://avlaw.com.au/cyberattacks-aviation-industry/ (accessed Apr. 30, 2021).

[5] IEC, "Defending airports against physical and cyber attacks | by IEC | e-tech | Medium," 2018. https://medium.com/e-tech/defending-airports-against-physical-and-cyber-attacks-fe1cbe30b2c9 (accessed Apr. 30, 2021).

[6] Volpe, "Improving Communications Between Pilots and Air Traffic Controllers | Volpe National Transportation Systems Center," 2021. https://www.volpe.dot.gov/safety-management-and-human-factors/improving-communication-between-pilots-and-controllers (accessed Apr. 30, 2021).

[7] Joanna Bailey, "Are Commercial Airliners At Risk Of Being Hacked? - Simple Flying," 2019. https://simpleflying.com/are-commercial-airliners-at-risk-of-being-hacked/ (accessed Apr. 30, 2021).

[8] Walker Jaroch, "The Wide World of Wi-Fi | Aviation Pros," 2020. https://www.aviationpros.com/engines-components/aircraft-airframe-accessories/cabin-communications/article/21147075/the-wide-world-of-wifi (accessed Apr. 30, 2021).

[9] Sarah Kamrau, "WI-FI IN AIRCRAFT: ARE WE SAFE FROM HACKER ATTACKS OR HIJACKING?," 2015. https://www.kontron.com/en/blog/security/wi-fi-in-aircraft (accessed Apr. 30, 2021).

[10] Pranjal Pande, "How Do In Flight Entertainment Systems Work? - Simple Flying," 2020. https://simpleflying.com/in-flight-entertainment-systems/ (accessed Apr. 30, 2021).

[11] Jim Sparks, "Avionics Technology: Cabin Entertainment Systems | Aviation Pros," 2005. https://www.aviationpros.com/home/article/10385684/avionics-technology-cabin-entertainment-systems (accessed Apr. 30, 2021).

[12] Elizabeth Weise, "Computer expert hacked into plane and made it briefly fly sideways, according to FBI | The Independent | The Independent," 2015. https://www.independent.co.uk/news/world/americas/computer-expert-hacks-plane-and-makes-it-fly-sideways-according-fbi-10256145.html (accessed Apr. 30, 2021).

[13] Sofia Tokar, "What is Air Traffic Control," 2018. https://www.snhu.edu/about-us/newsroom/2018/07/what-is-air-traffic-control (accessed Apr. 30, 2021).

[14] Małgorzata ŻMIGRODZKA, "View of Cybersecurity – One of the Greatest Challenges for Civil Aviation in the 21st Century | Safety & Defense," 2020. https://www.sd-magazine.eu/index.php/sd/article/view/73/60 (accessed Apr. 30, 2021).

[15] Aircraft systems tech, "Global Positioning System (GPS) in Aviation | Aircraft Systems." https://www.aircraftsystemstech.com/2017/05/global-positioning-system-gps.html (accessed May 01, 2021).

[16] Max eddy, "Satellite Communications Hacks Are Real, and They're Terrifying | PCMag," 2018. https://www.pcmag.com/news/satellite-communications-hacks-are-real-and-theyre-terrifying (accessed May 01, 2021).

[17] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "Air Traffic Communication Security," Trans. Intell. Transp. Syst., vol. 18, no. 6, pp. 1–20, 2016.

[18] Paul Marks, "Air traffic system vulnerable to cyber attack | New Scientist," 2011. https://www.newscientist.com/article/mg21128295-600-air-traffic-system-vulnerable-to-cyber-attack/ (accessed May 02, 2021).

[19] Brian Prince, "Air Traffic Control Systems Vulnerabilities Could Make for Unfriendly Skies [Black Hat] | SecurityWeek.Com," 2012.

https://www.securityweek.com/air-traffic-control-systems-vulnerabilities-could-make-unfriendly-skies-black-hat (accessed May 02, 2021).

[20] G. Markowsky, C. Giannatto, and G. Markowsky, “Potential Vulnerabilities of the NextGen Air Traffic Control System,” no. July 2014, 2014, [Online]. Available: https://www.researchgate.net/publication/294457234.

[21] Thomas Brewster, “This Guy Hacked Hundreds Of Planes From The Ground,” 2018. https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/?sh=394c818b46f2 (accessed May 02, 2021).

[22] Steve Weisman, “What Is a DDoS Attack? Distributed Denial-of-Service Attack Explained | Norton,” 2020. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html (accessed May 02, 2021).

[23] L. Ran, “Information Security Risks in Civil Aviation Network: Classification, Identification and Preventive Strategies,” DEStech Trans. Environ. Energy Earth Sci., no. peees, pp. 45–53, 2021, doi: 10.12783/dteees/peees2020/35463.

[24] Forbes Technology Council, “10 Cybersecurity Protocols Every Tech Professional Should Follow,” 2018. https://www.forbes.com/sites/forbestechcouncil/2018/11/28/10-cybersecurity-protocols-every-tech-professional-should-follow/?sh=f6914d63ae88 (accessed May 04, 2021).

[25] Trend Micro, “Cyberattacks from the Frontlines: Incident Response Playbook for Beginners - Security News,” 2020. https://www.trendmicro.com/vinfo/us/security/news/managed-detection-and-response/cyberattacks-from-the-frontlines-incident-response-playbook-for-beginners (accessed May 04, 2021).

[26] Touhid, “Different Types of Computer Security | Cyber Security Portal,” 2019. https://cyberthreatportal.com/types-of-computer-security/ (accessed May 04, 2021).

[27] E-Council, “What is STRIDE methodology in Threat Modeling?” https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling/ (accessed May 04, 2021).

[28] D. Fayez Alqushayri, “Cybersecurity Vulnerability Analysis and Countermeasures of Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems Commercial Aircraft Avionic Systems Scholarly Commons Citation Scholarly Commons Citation,” 2020. Accessed: May 02, 2021. [Online]. Available: https://commons.erau.edu/edt/519.

[29] L. Zhen, Y. Zhang, K. Yu, N. Kumar, A. Barnawi and Y. Xie, "Early Collision Detection for Massive Random Access in Satellite-Based Internet of Things," IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 5184-5189, May 2021, doi: 10.1109/TVT.2021.3076015.

[30] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, “A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things”, ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.

[31] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, “Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness”, IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.

[32] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang and T. Sato, “A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid,” IEEE Transactions on Instrumentation and Measurement, vol. 64, no. 8, pp. 2072-2085, August 2015.

[33] Arun, M., Baraneetharan, E., Kanchana, A. and Prabu, S., 2020. Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.

[34] Kumar, M.K., Parameshachari, B.D., Prabu, S. and liberata Ullo, S., 2020, September. Comparative Analysis to Identify Efficient Technique for Interfacing BCI System. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012062). IOP Publishing.

[35] Chowdary, M.K., Nguyen, T.N. and Hemanth, D.J., 2021. Deep learning-based facial emotion recognition for human–computer interaction applications. Neural Computing and Applications, pp.1-18.

[36] Sah, D.K., Nguyen, T.N., Cengiz, K., Dumba, B. and Kumar, V., 2021. Load-balance scheduling for intelligent sensors deployment in industrial internet of things. Cluster Computing, pp.1-13.

[37] Do, D.T., Van Nguyen, M.S., Nguyen, T.N., Li, X. and Choi, K., 2020. Enabling multiple power

beacons for uplink of noma-enabled mobile edge computing in wirelessly powered IOT. IEEE Access, 8, pp.148892-148905.

[38] Kumar, T.M., Reddy, K.S., Rinaldi, S., Parameshachari, B.D. and Arunachalam, K., 2021. A Low Area High Speed FPGA Implementation of AES Architecture for Cryptography Application. Electronics, 10(16), p.2023.

[39] Parameshachari, B.D., 2021, March. Logistic Sine Map (LSM) Based Partial Image Encryption. In 2021 National Computing Colleges Conference (NCCC) (pp. 1-6). IEEE.

[40] Kowsalya, T., Babu, R.G., Parameshachari, B.D., Nayyar, A. and Mehmood, R.M., 2021. Low Area PRESENT Cryptography in FPGA Using TRNG-PRNG Key Generation. CMC-COMPUTERS MATERIALS & CONTINUA, 68(2), pp.1447-1465.