"AI-Driven Cybersecurity Risks and Defense in Avionics Systems"

Prof. Devang Lakhani[1], Prof. Sudhanshu Srivastava[2]

[1]Department of Aeronautical Engineering, Parul University.
[2]Department of Aeronautical Engineering, Parul University.

---***---

Abstract - Advancements in the digitization and automation of critical infrastructures, particularly in aeronautical Communication, Navigation, and Surveillance (CNS) technologies, have led to the merging of complex physical and information networks with artificial intelligence (AI) systems. This integration has significantly enhanced the capabilities of avionics and Air Traffic Management (ATM) systems, improving data processing, information sharing, and geographic coverage. However, these advancements also make these systems more vulnerable to cybersecurity threats, physical weaknesses, and risks to data integrity. The interconnected nature of CNS infrastructure, together with ATM systems, increases the likelihood of widespread attacks, as threats can rapidly spread across connected components. Consequently, both ATM and UAS Traffic Management (UTM) systems are facing growing security challenges. Although the concept of cybersecurity in aviation is not new, integrating it seamlessly into aviation systems continues to pose significant difficulties. As AI technology improves operational efficiency and reliability within aviation systems, it has also become a key area for emerging cybersecurity threats. AI-driven intrusions and thefts are progressively replacing traditional attack methods, prompting researchers to propose defensive strategies based on AI technology. This paper critically examines the cybersecurity vulnerabilities and threats that could impact ATM and UTM systems. It categorizes potential threat actors based on their goals, motivations, and capabilities, and explores various attack methodologies based on AI technology, alongside their defensive countermeasures.

Key Words**:** Cybersecurity, Avionics, Autonomous Systems, Cyber Threats, Air Traffic Management (ATM), UAS Traffic Management (UTM), CNS+A

1.INTRODUCTION

In 2021, the European Air Traffic Management Computer Emergency Response Team (EATM-CERT) highlighted the rising cybersecurity risks within the global aviation industry. Their report revealed that, in 2020 alone, fraudulent websites were responsible for losses amounting to $1 billion. The 2023 report indicated that aviation-related cyber-attacks occur at a rate of at least 2.5 incidents per week, largely driven by ransomware attacks. Most of these incidents affected original equipment manufacturers (OEMs) and airspace users, with economic motives being the primary drivers.

In response to the increasing air traffic density and the need for improved transparency and reliability in airspace information sharing, the global integration of airspace systems has driven significant modernization efforts within the Air Traffic Management (ATM) system. The next-generation ATM is based on the CNS+A hybrid framework, integrating communication, navigation, and surveillance with modernized intelligent systems, including space-based signals. This transformation necessitates the shift from traditional analog systems to more sophisticated digital systems, especially as part of initiatives like NEXTGEN in the U.S. and Europe. These changes are underpinned by digital data networks and the System-wide Information Management (SWIM) framework, enabling real-time data sharing between aircraft, ground facilities, and other aircraft.

Furthermore, the increased use of Unmanned Aircraft Systems (UAS), particularly for commercial delivery purposes, has led to a rise in both manned and unmanned aerial systems operating in lower-altitude airspace. In anticipation of this shift, UAS Traffic Management (UTM) systems have been developed, with initiatives like NASA's UAM services and Europe’s U-Space working to manage UAS operations in urban airspaces. As these systems rely heavily on AI algorithms and autonomous navigation technology, both CNS+A and UAM services face growing cybersecurity risks, particularly as AI-powered threats replace traditional intrusion methods.

Furthermore, the increased use of Unmanned Aircraft Systems (UAS), particularly for commercial delivery purposes, has led to a rise in both manned and unmanned aerial systems operating in lower-altitude airspace. In anticipation of this shift, UAS Traffic Management (UTM) systems have been developed, with initiatives like NASA's UAM services and Europe’s U-Space working to manage UAS operations in urban airspaces. As these systems rely heavily on AI algorithms and autonomous navigation technology, both CNS+A and UAM services face growing cybersecurity risks, particularly as AI-powered threats replace traditional intrusion methods.

This paper aims to provide the ATM research community with an updated understanding of the cybersecurity risks in ATM and UTM systems, while advancing the integration of security measures into UAM services. The paper is structured into four sections: the first analyzes and classifies attack strategies, the second identifies potential threat actors, the third examines possible attack targets within ATM and UTM systems, and the fourth proposes AI-based defensive strategies.

2. CLASSIFICATION OF CYBER-ATTACKS

Cyber-attacks within the aviation industry primarily target information systems, with the potential to disrupt various components of the ATM and UTM infrastructures. These attacks typically manifest as data breaches, involving data manipulation. Network-based attacks are common, impacting both software and hardware components. Based on the data-centric nature of these attacks, we categorize the methods into three main types: data interception, data manipulation, and data interference.

Fig -1: Types of cyber attacks

1. **Data Interception**: This involves unauthorized access to sensitive information. Attackers often exploit weaknesses in encryption and authentication mechanisms to bypass security protocols, introducing malicious software like Trojan horses or viruses to compromise system data. Common methods of data interception include eavesdropping and man-in-the-middle (MITM) attacks, where attackers secretly monitor or alter communications between parties. The primary goals behind data interception can be to steal information or facilitate further attacks.

2. **Data Manipulation**: Data manipulation represents a serious threat to both virtual systems and physical networks, particularly in interconnected aviation systems. Attackers may exploit vulnerabilities in systems and protocols to modify or delete data, thus compromising system integrity. Techniques such as MITM attacks, GPS spoofing, and ADS-B message manipulation are common methods for carrying out data manipulation, with the intent to alter system functionality or mislead operators.

3. **Data Interference**: This involves flooding communication channels or data paths with false information, preventing the legitimate transmission or reception of data. Denial of Service (DoS) attacks are a typical example, where attackers overwhelm a system's capacity, leading to service outages. For instance, interference in avionics systems that disrupt GPS signals could lead to a loss of navigation capability for unmanned aerial systems (UAS), resulting in significant operational failures within UTM systems.

- **SECURITY THREAT AGENTS**

The increasing use of AI algorithms within ATM systems and the anticipated growth of Urban Air Mobility (UAM) are introducing new complexities and threats. Several types of malicious actors are capable of compromising the security of both ATM and UTM systems. Based on their operational goals and capabilities, these threat agents can be classified into three categories: low-risk, medium-risk, and high-risk.

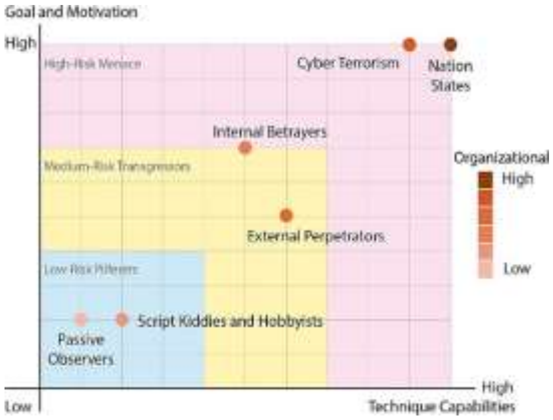

Fig -2: Classification of threat agents

- **Low-Risk Actors**: These individuals typically do not cause direct harm to the system but engage in data interception or surveillance activities for personal or recreational motives. Often referred to as "script kiddies" or hobbyists, they exploit existing vulnerabilities to gather data without malicious intent.

- **Medium-Risk Actors**: These actors may pose a moderate risk to the system by exploiting vulnerabilities for financial gain or other purposes. Their attacks may involve more sophisticated techniques such as data manipulation or distributed denial of service (DDoS) attacks.

- **High-Risk Actors**: High-level threats come from advanced persistent threats (APTs), state-sponsored actors, or criminal organizations with significant resources and technical expertise. These agents typically have broader goals, including espionage, sabotage, or large-scale disruption, and are capable of executing highly sophisticated attacks targeting both physical and digital infrastructure.

- **Medium-Risk Threat Actors:** Actors in this tier can wreak considerable havoc. They fall into two groups: **insiders** and **external attackers**. Insider threats—such as disgruntled employees or anyone with legitimate system privileges—can exploit their access or technical know-how to slip past defenses and exfiltrate data. Their motives range from personal grudge to pure profit, and their familiarity with internal processes makes them hard to spot.

  External cybercriminals, by contrast, scout for weaknesses in ATM and allied networks—via tactics like eavesdropping, signal jamming, or tampering with communications—and aim squarely at financial gain through stolen data. Backed by significant resources and expertise, they frequently deploy ransomware and extortion schemes, threatening extensive damage to force payouts. Expect these groups to remain the dominant "mid-level" threat in the years ahead.

- **High-Risk (Nation-Scale) Threat Entities** At the extreme end are those whose actions imperil national security and public order, causing catastrophic losses. Modern cyber-terrorists, extremist cells, and insurgents now leverage cutting-edge civil and military IT to strike aviation systems at their core. Their objectives include crippling ATM infrastructures and aviation control networks.
  Tactics range from drone-based reconnaissance and extremist propaganda to outright aerial attacks. In urban centers, weaponized drones can sow mass panic by targeting crowded locales. As Mwiki documents, state-sponsored hacker syndicates—armed with virtually boundless funding and deep expertise in ATM/UTM and avionics—have long operated under this banner. Their intimate system knowledge lets them bypass redundant safeguards, intercept data, disrupt networks, or even physically damage infrastructure to fulfill political and military goals.

- **AI-Driven Defenses**

Machine learning (ML) and related AI techniques are being enlisted to guard ATM/UTM systems against the very threats outlined above:

- **SVM-based GPS-spoofing detectors** compare inertial vs. satellite readings to spot anomalies without extra hardware.

- **ANN classifiers** trained on genuine versus tampered signals can flag attacked GPS streams with high accuracy and low false alarms—suitable even for small UAVs.

- **Ensemble-learning network forensics** can sift malware traffic and identify botnets, detecting DoS/DDoS attacks in real time.

- **GAN-powered adversarial simulators** (e.g. DoS-WGAN) generate realistic attack patterns to continually harden NIDS and other defenses.

Reinforcement-learning path planners enable drones to reroute autonomously if hijacking or jamming occurs mid-flight.

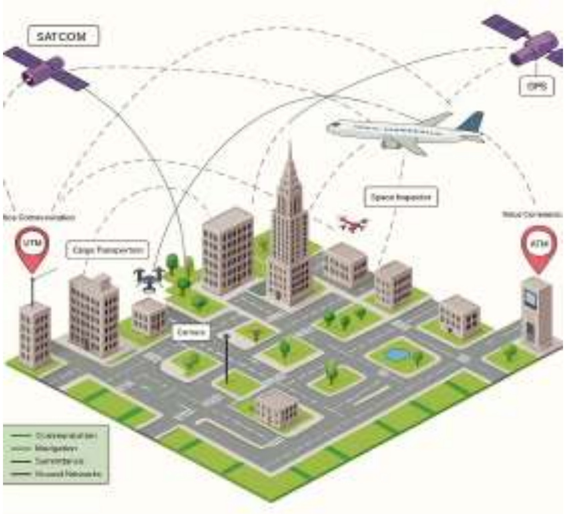

Fig -3: ATM and UTM system infrastructure in the CNS+A framework.

3. CONCLUSIONS

As aviation embraces ever more digital systems—particularly with UTM on the horizon—cyber risks will only intensify. A layered defense combining traditional cybersecurity measures with AI-augmented detection and response will be essential to maintain safety, integrity, and resilience in the skies.

ACKNOWLEDGEMENT

We, would like to express my deepest gratitude to all those who have supported and contributed to the completion of this research on AI-driven cybersecurity risks and defenses in avionics systems.

REFERENCES

1. Baldonado, M., Chang, C.-C.K., Gravano, L., Paepcke, A.: The Stanford Digital Library Metadata Architecture. Int. J. Digit. Libr. 1 (1997) 108–121
2. Bruce, K.B., Cardelli, L., Pierce, B.C.: Comparing Object Encodings. In: Abadi, M., Ito, T. (eds.): Theoretical Aspects of Computer Software. Lecture Notes in Computer Science, Vol. 1281. Springer-Verlag, Berlin Heidelberg New York (1997) 415–438
3. van Leeuwen, J. (ed.): Computer Science Today. Recent Trends and Developments. Lecture Notes in Computer Science, Vol. 1000. Springer-Verlag, Berlin Heidelberg New York (1995)
4. Michalewicz, Z.: Genetic Algorithms + Data Structures = Evolution Programs. 3rd edn. Springer-Verlag, Berlin Heidelberg New York (1996)

BIOGRAPHIES

Devang, a graduate with a Bachelor of Engineering in Aeronautical Engineering from SVIT, Vasad, is currently serving at Parul University in the PIET-DS Aeronautical Department. He is actively engaged in research centered on AI-driven cybersecurity risks and defense mechanisms within avionics systems. His work plays a crucial role in bridging advanced technological developments with aviation safety.

Sudhanshu, currently pursuing a Ph.D. in Aeronautical Engineering from Parul University, has a keen interest in aerospace systems. He is focused on research and hands-on learning. Passionate about innovation, he actively engages in technical projects. His goal is to contribute to advancements in aviation technology.

Description about the author1
(in 5-6 lines)