A Systematic Review of IoT Applications in Aviation: Enhancing Safety, Efficiency, and Smart Operations

JONAH GONZALO
Institute of Computer Studies
Philippine State College of Aeronautics
Fernando Air Base, Lipa City, Batangas
PHILIPPINES

Abstract: The integration of the Internet of Things (IoT) technologies is the one responsible for building the aviation industry by improving safety, the efficiency of how the aviation industry operates, and a system covering all different kinds of processes. This study presents a systematic literature review that tries to understand the diverse applications of IoT in terms of aviation processes, including predictive maintenance, smart airport operations, air traffic management, and supply chain optimization. A comprehensive search was conducted of major academic databases such as IEEE Xplore, ScienceDirect, SpringerLink, Scopus, Web of Science, Google Scholar, ResearchGate, and the ACM Digital Library to identify relevant peer-reviewed literature published primarily between 2018 and 2023. The studies mentioned were analyzed using a qualitative approach to analyze their content. It enables the identification of common technological components, reported benefits, and recurring challenges like cybersecurity risks, managing data complexities, and interoperability issues. The study revealed that even though the literature review shows a potential of IoT in aviation, there is still a need for further empirical research, regular development, and collaboration of sectors to provide a solution for the technical and organizational barriers in the aviation industry. This study contributes a timely and integrated perspective to support future innovation and policy formulation in the aviation technology landscape.

Keywords: Air Traffic Management, Aviation Technology, Internet of Things (IoT), Predictive Maintenance, Smart Airports

Received: July 14, 2025. Revised: October 12, 2025. Accepted: October 13, 2025. Published: October 14, 2025.

1 Introduction

Aviation, one major sector of the world economy and a key enabler of global connectivity, is being undergoing a radical change caused by the penetration of Internet of Things (IoT) [1],[2],[3]. This new paradigm is defined by the interconnectedness of numerous aircraft and aviation systems that together produce enormous amounts of data, which can be employed if utilized meaningfully to enhance safety, efficiency, and operational performance more broadly, on a substantial scale [1], [4], [5]. The development of smart airports, using technologies that include the Internet of Things (IoT) applied to the aviation field, is a clear result of this change [1]. These smart airports utilize IoT services and applications for performance improvement, efficiency, and control by using real-time monitoring and analytics, and facilitating passenger actions, which further enhances the security of the airport [1]. Although this real-time interaction increases connectivity, it also heightens the risk of security issues [1], [2], [6], necessitating the development of reliable security solutions to mitigate this risk. This review explores the applications of IoT in aviation in many ways, such as implications on the industry: maintenance of aircraft, air traffic control, airport operations, and supply chain management. IoT-enabled aviation is not just an evolution of existing benefits but a revolution in the way future aviation will become safer, more economical, and with a better passenger experience [7], [4], [8].

The significance of IoT in aviation stems from its potential to address some of the industry's most pressing challenges, namely enhancing safety and increasing efficiency. Traditional practices in aviation are often reactive, addressing issues only after they have occurred. The application of IoT enables a proactive approach by predicting and preventing potential problems before they escalate into actual incidents or disruptions. [9], [10], [3]. Continuous data collection from sensors on aircraft, at airports, and within air traffic control systems offers an unprecedented view of system performance, grounded in real-time operations [1], [4], [11]. This data-driven insight supports more informed decision-making and optimizes resource allocation. [1], [4], [11]. This transition towards a data-centric approach is significant to increase safety and efficiency in the aviation ecosystem as a whole [3], [7]. The giant amount of data resulting from these systems raises a serious challenge [11], [10]. The proper management, analysis, and learning from such data demands the use of sophisticated tools for storing such large trip data and advanced analytics methods [11], [9].

2 Methodology

This paper adopts a systematic literature review approach to explore the application of Internet of Things (IoT) technologies within the aviation sector, particularly concerning safety, operational efficiency, and system management. The methodology is structured around four key stages: identifying relevant literature, extracting and analyzing data, conducting comparative evaluations, and synthesizing the findings. Additionally, a separate paragraph discusses the study's limitations to provide a balanced perspective on the scope and reliability of the results.

2.1 Literature Collection

Relevant academic databases were searched in 2023 for relevant academic papers in a scoping review. The databases utilized include:

- IEEE Xplore Digital Library
- ScienceDirect (Elsevier)
- SpringerLink
- Scopus
- Web of Science
- Google Scholar
- ResearchGate
- ACM Digital Library

The literature review mainly comprises articles from 2010 onwards, focusing on the period of 2018-2023. This span was selected to reflect the latest technology trends, newer developments, as well as persistent challenges related to the IoT in aerospace. Prior studies published before 2010 were included if they contributed theoretical or conceptual models related to current practice.

Search term combinations used for keyword-based search include "IoT in aviation", "smart airports", "aircraft maintenance", "air traffic management", "aviation supply chain", etc. Peer-reviewed journal papers, conferences, and industry reports related to the use-cases, benefits, implementation barriers, and the future of IoT in the aviation domain were targeted, but not limited to.

2.2 Data Extraction and Analysis

Relevant information was systematically extracted from the selected sources to capture the following key aspects:

- There are a number (such as predictive maintenance, air traffic management, smart airport operations, etc.) of different types of IoT applications.
- Key technology elements (sensors, UAVs, RFID, digital twins, blockchain)
- Reported benefits and operational improvements.
- Challenges that have been identified, such as those posted by cybersecurity, data management, interoperability, and regulatory issues, can be addressed by systems that allow healthcare to occur anywhere at any time.

Data was coded using a qualitative content analysis to group responses, highlight patterns, and make sense of cross-cutting elements. This method allowed identifying the lack of knowledge and the development of more comprehensive views regarding the use of IoT integration in aviation.

2.3 Comparative Evaluation

The eligible studies were compared under the categories of research design, technological emphasis, and empirical results.

This side-by-side comparison allowed the analysis of the various IoT deployment approaches and revealed patterns in the challenges, enablers, and sector-specific best practices encountered in the aviation ecosystem.

2.4 Synthesis and Framework Development

Findings based on the literature were synthesized to develop the conceptual framework regarding several applications of IoT for aviation, the connections among these applications, and the significant factors affecting successful usage. The proposed framework is designed as a tutorial guide for future studies and industry implementations.

2.5 Limitations

Limitations of the review are shaped by the scope and lack of literature. It only shows that it is driven by secondary data and may not reflect recent developments in industry practice. Future empirical research, pilot projects, and longitudinal case studies are needed to test and extend the ideas introduced in this review.

3 Literature Review

A. Applications of IoT in Aviation

The applications of IoT in aviation are diverse and far-reaching, impacting various aspects of the industry. These applications can be broadly categorized into:

1. *Aircraft Maintenance:* Predictive maintenance facilitated through onboard sensor data analysis allows a timely detection and takes actions against potential issues before they result in downtime or safety hazards [9], [10]. The systematic use of UAVs combined with infrared cameras and RFIDs progressively improves efficiency and accuracy in aircraft inspections [10]. The Digital Twin paradigm, which is a computer-based model of an aircraft updated with real-time data that spans the flight life of the vehicle, offers a robust approach for the simulation of different scenarios and for the optimal planning of a maintenance activity [9].

2. *Air Traffic Management:* The growing intensity of air traffic and the spread of UAVs call for the enforcement of more reliable, efficient air traffic management [12]. It is admitted that the IoT can be used to build new and efficient air traffic management systems, which are more interconnected and data-rich, and capable of monitoring and controlling the airspace in a real time way: this, from one side, can lead to improve safety, from the other hand, increase efficiency [12].

4. *Airport Operations:* With the help of IoT, smart airports are able to manage different types of operations such as passenger processing, baggage handling, security control, movement management, and environmental management [1], [2]. With real-time data analytics, airport administrations can optimize resource assignment, passenger flow, and achieve higher operational efficiency [1], [2].

4. *Aviation Supply Chain Management*: The aviation supply chain is complicated, from the procurement and distribution to the maintenance of an enormous number of parts of an airplane. IoT can also increase transparency and traceability along the chain, thus enabling cost savings and efficiency improvement [13], [14]. Blockchain technology may additionally be used to improve security and to prevent counterfeiting [13].

B. Challenges of IoT Implementation in Aviation

Despite the significant potential benefits, the implementation of IoT in aviation faces several challenges:

1. *Cybersecurity:* The very distributed nature of IoT-based systems forms a wide attack surface to be attacked by several cyber threats [1], [2], [6]. To secure sensitive information and maintain the integrity of essential services, strong cybersecurity measures are necessary [1], [2], [6]. The growing complexity of cyber-threats requires more sophisticated cyber-defense strategies, as well as AI-supported security products [1].

2. *Data Management and Analytics:* The amount of data in aviation can be big because of IoT devices; there must be robust data management systems and advanced analytic methods [11], [10]. Efficiently managing, storing, and analyzing such massive data is a challenging task [11], [9]. Efficient algorithms

and data pre-processing techniques are the main requirement for real-time data analysis to be possible [11].

3. *Communication Technologies:* Selection of the communication technology is one of the key factors in the successful deployment of IoT in aviation [15]. Various applications have different demands in bandwidth, delay, power consumption, and security [15]. Combining various communication technologies and protocols may be required for complete connectivity in aviation IoT [15].

4. *Interoperability:* Achieving an effective data communication among systems and platforms necessitates generating standard data formats and an interoperability protocol [13], [14]. Non-standardization of wireless devices inhibits the integration of IoT devices from multiple vendors and causes cross-interoperability problems [13], [14].

5. *Regulatory Framework:* With the accelerated growth of IoT devices and services, appropriate regulatory measures are needed not only to ensure safety and security but also to protect the privacy [12], [2]. These frameworks must tackle security concerns, data privacy challenges, and the inclusion of new technologies under the traditional aviation regulation [12], [2].

C. IoT Applications in Aircraft Maintenance

The use of the IoT and aircraft maintenance leads a critical conversion from reactive maintenance to proactive and predictive strategies [9], [10]. Contemporary aircraft are fitted with numerous sensors, which are estimated to produce about terabytes of data per flight [7]. Such streaming data can give real-time feedback regarding the status of the aircraft and the performance of its multiple parts. With this data, and sophisticated fusion algorithms and machine learning tools that can be applied to analyze the state of the system, the prediction of possible failures before they happen is feasible [9], [10]. The proactive strategy not only decreases production loss, maintenance cost but also has a tremendous impact on safety by (potentially) preventing catastrophic incidents [9], [10].

The implementation of an Infrared UAV-based and RFID-technology-assisted aircraft inspection system is a significant breakthrough in aircraft inspection [10]. Unmanned Aerial Vehicles can reach inaccessible surfaces of aircraft, inspecting them in a more comprehensive and accurate manner than other methods, such as visual inspection, which are used at the present time [10]. Infrared cameras can be used to identify small heat anomalies, which may be a sign of a problem, and RFID can be used to identify and track an aircraft part down to the serial number [10]. Integration of these techniques enhances the accuracy and the efficiency of aircraft inspection and allows for better maintenance decisions [10].

The concept of the Digital Twin [9] further enhances the capabilities of predictive maintenance. A Digital Twin is a virtual representation of a physical asset, in this case, an aircraft, that is constantly updated with real-time data from various sensors [9]. Such a model can be used to simulate different conditions and predict possible cases of failure under different operation conditions [9]. Furthermore, cybersecurity concerns are paramount, as the interconnected nature of these systems makes them vulnerable to cyberattacks [9]. The integration of AI and machine learning techniques is crucial for effectively analyzing the vast amounts of data generated by these systems and extracting actionable insights [9].

However, there are challenges for IoT in aircraft maintenance as well. The large amount of data generated demands strong data management systems and sophisticated analytical capabilities [9]. Real-time analysis and processing of data are now required to produce efficient algorithms and high-performance computing infrastructure [9]. And also, cybersecurity is critical; the interconnected systems are facing the threat of being attacked [9]. Protecting the integrity of maintenance data and preventing malicious interference is crucial for ensuring the safety and reliability of aircraft operations [9].

D. IoT in Air Traffic Management: Enhancing Safety and Efficiency

The increasing complexity of air traffic, particularly with the integration of Unmanned Aerial Vehicles (UAVs) into the airspace, necessitates a more sophisticated and robust air traffic management (ATM) system [12]. Traditional ATM systems often struggle to handle the high volume and density of air traffic, particularly in urban environments [12]. The integration of IoT technologies offers the potential to create a more interconnected and data-rich ATM system, enabling real-time monitoring and control of air traffic, thereby improving safety and efficiency [12].

A multilayer network model, for example, could be used to represent the airspace as a network of interconnected nodes and airways, with each node representing an aircraft or UAV and each airway representing a flight path [12]. This model allows for the simulation of various scenarios and the optimization of air traffic flow, minimizing the risk of collisions and maximizing airspace utilization [12]. Real-time data from various sensors, including onboard aircraft systems, ground-based radar, and weather stations, can be integrated into this model to provide a comprehensive and dynamic picture of the airspace [12].

The use of IoT technologies in ATM also enables the development of advanced decision support systems that can assist air traffic controllers in making informed decisions in real-time [12]. These systems can analyze vast amounts of data to identify potential conflicts, predict delays, and optimize air traffic flow [12]. The integration of AI and machine learning techniques can further enhance the capabilities of these decision support systems, enabling them to adapt to changing conditions and learn from past experiences [12].

However, the integration of IoT in ATM also presents significant challenges. The sheer volume of data generated requires robust data management and processing capabilities [12]. Ensuring the reliability and security of communication networks is crucial for the safe and efficient operation of the ATM system [12]. The development of robust and scalable algorithms capable of handling high traffic demands is essential for the successful implementation of IoT-based ATM systems [12]. Furthermore, the integration of IoT devices into ATM systems raises cybersecurity concerns, as these systems become potential targets for malicious actors [12]. Robust cybersecurity measures are crucial for protecting the integrity and reliability of the ATM system [12].

E. IoT in Smart Airports: Enhancing Passenger Experience and Operational Efficiency

Intelligent airports utilize IoT devices to increase operational efficiency, and improve passenger experience and security [1], [2]. The widespread use of smart sensors integrated in airports of multiple characteristics enables the real-time control of environmental conditions in the airport, passenger flow, and helicopter baggage [1], [2]. When integrating these data with advanced analytics methods, it can assist airport authorities to make the most efficient use of their resources, optimize passenger flow, and boost security measures [1], [2].

Automation of different airport functions, such as baggage handling and security screening, results in low costs and higher efficiency [1], [2]. Real-time tracking of baggage allows for quicker and more efficient baggage delivery, reducing delays and improving passenger satisfaction [1], [2]. Through smart sensors, we can monitor the surroundings and detect potential threats and send alerts to the security personnel to improve the safety of the airport, and in addition, for quick response to incidents [1], [2].

Furthermore, the implementation of IoT in smart airports enhances passenger experience by facilitating the dissemination of real-time flight status, gate allocation, as well as amenities [1], [2]. With the help of mobile apps, passengers can travel at the airport, be informed about the available services around the airport, and support ease of travel [1], [2]. Data analytics can provide airport management with the tools to better manage resources (e.g., personnel and equipment) to meet passenger needs more efficiently [1], [2].

However, smart airports adopting IoT are facing tremendous challenges. These systems are networked entities, and this makes them susceptible to malicious cyberattacks, which can lead to disruptions in services, unauthorized access to private information, and even threaten passenger safety and system operation [1], [2]. Strong cybersecurity is critical to safeguarding the integrity and availability of airport systems [1], [2]. The vast amounts of data collected by IoT devices are beyond the ability of many data management and analytics systems to cope with [1],[2]. Incorporating all these different systems and technologies requires careful planning to establish good interoperability and seamless operations [1], [2].

F. IoT and Aviation Supply Chain Management: Enhancing Traceability and Efficiency

The aviation industry's supply chain is intricate and globally dispersed, encompassing the procurement, distribution, and maintenance of thousands of aircraft parts [13], [14]. Existing practices in supply chain management (which are typically based on bulky information systems) do not always support a response to the exact location and status of these parts in real time, which means productivity is compromised [13], [14]. Adoption of IoT into this sector can change the scenario completely, for it enables real-time tracking and monitoring of aircraft parts in the supply chain [13], [14].

RFID tags and IoT sensors can monitor the whereabouts and condition of aircraft parts throughout the supply chain, from the production line to installation [13], [14]. This increased visibility helps to manage the inventory in a fine way and finally to reduce storage costs and logistics [13], [14]. Real-time data on part location and condition enables proactive maintenance and reduces the risk of delays caused by part shortages [13], [14].

The use of Blockchain also improves the security and transparency of the aviation supply chain [13]. The enhanced transparency and traceability attributed to the blockchain technology promote trust among the involved parties and ease the supply chain process [13]. However, the implementation of IoT and blockchain in aviation supply chains also presents challenges. The interoperability between different systems and technologies must be carefully planned and coordinated [13], [14]. Cybersecurity concerns are to be considered since the interconnection of these systems exposes them to cyberattacks [13], [14]. It is imperative to build secure mechanisms for protecting sensitive information to provide security and integrity for the supply chain [13], [14]. Another challenge for the adoption of IoT and blockchain is the high cost of deployment, which can be a particularly strong deterrent for smaller companies [13], [14].

G. Communication Technologies in Aviation IoT: A Comparative Analysis

The successful implementation of IoT in aviation relies heavily on the availability of reliable and efficient communication technologies [15], [6]. Various communication technologies are employed, each with its strengths and limitations. Narrowband Internet of Things (NB-IoT) technology is particularly well-suited for low-power applications, such as sensors embedded within aircraft [15]. NB-IoT's low power consumption and extended battery life make it ideal for applications where power is a critical constraint [15]. However, NB-IoT's limited bandwidth may not be sufficient for applications requiring high data rates, such as real-time video streaming [15].

The successful implementation of IoT in aviation relies heavily on the availability of reliable and efficient communication technologies [15], [6]. Different types of communication technologies are used, with their respective advantages and disadvantages. The narrowband internet of things (NB-IoT) is specifically tailored to low-power constraints, as for the sensors inside the plane [15]. NB-IoT's low power consumption and extended battery life make it ideal for applications where power is a critical constraint [15]. However, the narrow bandwidth of Narrowband (NB)-IoT may not be enough for applications that need high-rate data transmission, for example, real-time video streaming [15].

G technologies such as 5G provide far more bandwidth and lower latency; hence, they are suitable for high bandwidth and latency-demanding applications [15]. The excellent capacity for massive connection has made 5G an enabler for massive IoT applications [15]. Nevertheless, 5G has higher power consumption than NB-IoT, which could prevent 5G from being used in some low-power-limited scenarios [15].

The selection of communication technology depends on the specific application requirements, considering factors such as bandwidth, latency, power consumption, and security [15], [6]. To strike a fully interconnected aviation IoT ecosystem, some of these communication technologies and protocols can be integrated [15], [6]. For instance, low-bandwidth sensor data transmissions might be served well by NB-IoT, and the high-bandwidth applications, such as real-time video applications, might be served by 5G [15], [6]. It is essential to develop secure communication protocols to protect this sensitive information accessed over these networks [15], [6]. The use of advanced encryption techniques and authentication protocols is essential for mitigating cybersecurity risks [15], [6].

H. Cybersecurity Challenges and Mitigation Strategies in Aviation IoT

The increasing reliance on IoT technologies in aviation introduces significant cybersecurity risks [1], [2], [6]. The interconnected nature of these systems creates a large attack surface, making them vulnerable to a wide range of cyber threats [1], [2], [6]. These threats can range from relatively benign denial-of-service attacks to more sophisticated attacks that could compromise the safety and security of aircraft and passengers [1], [2], [6].

Identity spoofing attacks, where malicious actors mimic legitimate devices to gain unauthorized access to systems, pose a significant threat [6]. Advanced Persistent Threats (APTs), which involve prolonged and targeted attacks aimed at gaining persistent access to systems, also pose a serious risk [1]. Data breaches, resulting in the unauthorized access and disclosure of sensitive information, can have severe consequences for both individuals and organizations [1].

To mitigate these risks, robust cybersecurity measures are essential [1], [2], [6]. These measures should include advanced encryption techniques to protect sensitive data, intrusion detection systems to monitor network traffic for malicious activity, and regular security audits to identify and address vulnerabilities [1], [2], [6]. The development and implementation of secure communication protocols and data exchange standards are crucial for reducing the vulnerability of IoT systems [1], [2], [6].

The integration of AI-based security solutions can enhance the detection and prevention of cyber threats [1], [2], [6]. AI algorithms can analyze large volumes of data to identify patterns and anomalies indicative of malicious activity, providing real-time protection against evolving attack vectors [1], [2], [6]. The development of AI-enabled security systems is crucial for addressing the increasing sophistication of cyberattacks and ensuring the safety and security of IoT-enabled aviation systems [1], [2], [6].

I. Data Management and Analytics in Aviation IoT

The integration of IoT in aviation generates massive amounts of data, requiring robust data management and analytics capabilities [11], [10]. Effective data management systems are essential for storing, processing, and analyzing this data, extracting valuable insights for improved decision-making [11], [10]. Advanced analytics techniques, such as machine learning and deep learning, can be employed to identify patterns and anomalies in this data, enabling predictive maintenance, optimized resource allocation, and enhanced safety measures [11], [10].

The development of effective data analytics solutions requires careful consideration of several factors, including data quality, data security, and the scalability of the analytics infrastructure [11], [10]. Data quality is crucial for ensuring the reliability of analytical results [11], [10]. Data security is paramount for protecting sensitive information from unauthorized access and disclosure [11], [10]. The scalability of the analytics infrastructure is essential for handling the large volume of data generated by IoT devices in real-time [11], [10].

The use of cloud computing platforms can provide the necessary scalability and processing power for managing and analyzing this data effectively [11], [10]. Cloud computing platforms offer flexible and scalable infrastructure that can adapt to changing data volumes and processing requirements [11], [10]. They also provide access to advanced analytics tools and services that can be used to extract valuable insights from aviation data [11], [10].

However, the use of cloud computing also raises cybersecurity concerns [11], [10]. Protecting sensitive data stored in the cloud requires robust security measures, including encryption, access control, and regular security audits [11], [10]. The selection of a secure and reliable cloud provider is crucial for ensuring the confidentiality and integrity of aviation data [11], [10].

J. Research Gaps and Future Directions in Aviation IoT

Despite the significant progress made in the integration of IoT in aviation, several research gaps remain. Further research is needed to address the cybersecurity challenges associated with IoT implementation, developing robust and adaptable security protocols and mitigation strategies [1], [2], [6]. The development of efficient data management and analytics solutions capable of handling the massive amounts of data generated by IoT devices is also crucial [11], [10].

Research into the development of more energy-efficient communication technologies, such as NB-IoT and 5G, is necessary to support the widespread deployment of IoT devices in aviation [15]. Further investigation into the integration of AI and machine learning techniques for real-time anomaly detection and predictive maintenance is also crucial [9]. The development of standardized data formats and interoperability protocols will be essential for ensuring seamless data exchange between different systems and platforms [13], [14].

Further research is also needed to explore the ethical and societal implications of IoT in aviation [16]. Concerns about data privacy, algorithmic bias, and the potential displacement of human workers require careful consideration [16]. The development of regulatory frameworks that address these concerns is crucial for ensuring the responsible and sustainable development of IoT in aviation [16]. A multidisciplinary approach, involving researchers from various fields, including computer science, engineering, law, and social sciences, is essential for addressing the complex challenges associated with the integration of IoT in aviation [16].

4 Results and Discussion

The literature review highlights the significant role of Internet of Things (IoT) technologies in transforming the aviation industry by enhancing operational efficiency, safety, and decision-making. Key areas of application include aircraft maintenance, air traffic management, airport operations, and supply chain management, each benefiting from real-time data analytics and increased automation.

Predictive maintenance, enabled by data from onboard sensors and advanced analytical tools, emerged as a crucial innovation. This approach reduces unplanned downtime and improves aircraft reliability by identifying issues before they escalate into failures [9], [10]. The integration of UAVs with infrared cameras and RFID technologies supports detailed inspection and monitoring, particularly in inaccessible components of the aircraft, enhancing diagnostic accuracy [10]. Complementing this is the Digital Twin concept, a dynamic virtual representation of an aircraft that enables simulation-based maintenance planning and performance analysis [9].

In air traffic management, the literature underscores IoT's capacity to manage complex airspaces, especially with the rise of unmanned aerial vehicles through enhanced connectivity, data fusion, and multilayer models that support real-time monitoring and decision-making [12]. Despite these benefits, issues such as data volume, reliability of communication networks, and system scalability are identified as barriers to implementation [12].

Smart airport operations also benefit from IoT through improved passenger flow management, security procedures, and baggage handling. By leveraging sensor data and automation, airports can enhance efficiency and passenger satisfaction [1], [2]. However, the widespread integration of IoT systems increases vulnerability to cybersecurity threats, which necessitates robust security frameworks, AI-enabled threat detection, and encrypted communications [1], [2], [6].

In the context of aviation supply chain management, IoT provides end-to-end visibility through real-time tracking of parts using RFID and sensor networks. This enhances traceability, reduces losses, and optimizes inventory systems [13], [14]. The incorporation of blockchain technology further strengthens transparency and trust in the authenticity of aviation components [13]. Nevertheless, the lack of interoperability standards and fragmented systems hinders seamless integration across different platforms [14].

Cybersecurity and data management emerge as overarching challenges across all domains. The literature emphasizes that the large-scale deployment of interconnected devices significantly expands the attack surface, exposing aviation systems to a range of cyber threats [1], [2], [6]. In parallel, the immense volume of data generated necessitates high-performance computing infrastructure and advanced analytics capabilities for real-time processing and decision-making [11].

Lastly, regulatory and communication frameworks lag behind the rapid evolution of IoT technologies. The successful deployment of IoT in aviation depends not only on technical innovation but also on the development of standardized communication protocols, interoperability measures, and adaptive regulatory mechanisms [12], [13], [14].

In summary, the literature affirms that IoT is a transformative force in aviation, with wide-ranging applications that contribute to safety, efficiency, and strategic planning. However, realizing its full potential requires collaborative efforts to address cybersecurity, data governance, technical integration, and policy development.

5 Conclusion

The integration of IoT technologies in aviation is poised to revolutionize the industry, offering significant potential for enhancing safety, improving efficiency, and transforming the passenger experience. While the benefits are substantial, several challenges remain, particularly in the areas of cybersecurity, data management, communication technologies, and interoperability. Addressing these challenges requires a collaborative effort between industry stakeholders, researchers, and policymakers, focusing on the development of robust, secure, and interoperable systems that can meet the unique demands of this complex and safety-critical environment. The continued advancements in sensor technology, communication protocols, data analytics, and cybersecurity will shape the future of aviation, paving the way for a safer, more efficient, and more connected industry. The potential for continuous improvement through data-driven insights and automated processes points towards a future where IoT plays an increasingly integral role in maintaining the highest standards of safety and operational excellence in aviation.

References

[1] Koroniotis, Nickolaos & Moustafa, Nour & Schiliro, Francesco & Gauravaram, Praveen & Janicke, Helge. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access. 8. 209802-209834. 10.1109/ACCESS.2020.3036728.

[2] Lykou, Georgia, Argiro Anagnostopoulou, and Dimitris Gritzalis. 2019. "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls" *Sensors* 19, no. 1: 19. https://doi.org/10.3390/s19010019

[3] Dou, Xiangsheng. 2020. "Big Data and Smart Aviation Information Management System." *Cogent Business & Management* 7 (1). doi:10.1080/23311975.2020.1766736.

[4] Ushakov, D., Dudukalov, E., Kozlova, E., & Shatila, K. (2022). The Internet of Things impact on smart public transportation. *Transportation Research Procedia*, *63*, 2392–2400. https://doi.org/10.1016/j.trpro.2022.06.275

[5] Perwej, Y., Haq, K., Parwej, F., & M, M. (2019). The Internet of Things (IoT) and its Application Domains. *International Journal of Computer Applications*, *182*(49), 36–49. https://doi.org/10.5120/ijca2019918763

[6] Liu, Yongxin & Wang, Jian & Li, Jianqiang & Song, Houbing & Yang, Thomas & Niu, Shuteng & Ming, Zhong. (2020). Zero-Bias Deep Learning for Accurate Identification of Internet of Things (IoT) Devices. 10.48550/arXiv.2009.02267.

[7] Valdés, Rosa Arnaldo, Víctor Fernando Gómez Comendador, Alvaro Rodriguez Sanz, and Javier Perez Castán. 2018. ‘Aviation 4.0: More Safety through Automation and Digitization’. Aircraft Technology. InTech. doi:10.5772/intechopen.73688.

[8] Ping H, Wang J H, Ma Z H, Du Y F. Mini-review of application of IoT technology in monitoring agricultural products quality and safety. Int J Agric & Biol Eng, 2018; 11(5): 35–45.

[9] Liu, Z., Meyendorf, N., & Mrad, N. (2018). The role of data fusion in predictive maintenance using digital twin. *AIP Conference Proceedings*. https://doi.org/10.1063/1.5031520

[10] Hrúz, Michal, Martin Bugaj, Andrej Novák, Branislav Kandera, and Benedikt Badánik. 2021. "The Use of UAV with Infrared Camera and RFID for Airframe Condition Monitoring" *Applied Sciences* 11, no. 9: 3737. https://doi.org/10.3390/app11093737

[11] Wang, W., Fan, L., Huang, P., & Li, H. (2019). A new data processing architecture for Multi-Scenario applications in aviation manufacturing. *IEEE Access*, *7*, 83637–83650. https://doi.org/10.1109/access.2019.2925114

[12] Samir Labib, Nader, Grégoire Danoy, Jedrzej Musial, Matthias R. Brust, and Pascal Bouvry. 2019. "Internet of Unmanned Aerial Vehicles—A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management" *Sensors* 19, no. 21: 4779. https://doi.org/10.3390/s19214779

[13] Madhwal, Y., & Panfilov, P. (2017). Blockchain and Supply chain Management: Aircrafts’ parts’ business case. In *Annals of DAAAM for . . . & proceedings of the . . . International DAAAM Symposium* (pp. 1051–1056). https://doi.org/10.2507/28th.daaam.proceedings.146

[14] Khan, Yasser, Mazliham Bin Mohd Su’ud, Muhammad Mansoor Alam, Syed Fayaz Ahmad, Ahmad Y. A. Bani Ahmad (Ayassrah), and Nasir Khan. 2023. "Application of Internet of Things (IoT) in Sustainable Supply Chain Management" *Sustainability* 15, no. 1: 694. https://doi.org/10.3390/su15010694

[15] S. Duhovnikov, A. Baltaci, D. Gera and D. A. Schupke, "Power Consumption Analysis of NB-IoT Technology for Low-Power Aircraft Applications," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 719-723, doi: 10.1109/WF-IoT.2019.8767234. keywords: {Aircraft;Batteries;Temperature sensors;Long Term Evolution;Power demand;Temperature measurement;NB-IoT;Power Consumption;Battery Life;PSM},

[16] Nikitas, Alexandros, Kalliopi Michalakopoulou, Eric Tchouamou Njoya, and Dimitris Karampatzakis. 2020. "Artificial Intelligence, Transport and the Smart City: Definitions and Dimensions of a New Mobility Era" *Sustainability* 12, no. 7: 2789. https://doi.org/10.3390/su12072789