Mediterranean Smart Cities Conference (MSCC 2024)
2-4 May 2024, Martil, Morocco

Advancements in Airport Security Technologies: A Patent Analysis

Mahmoud ELEIMAT
Doctoral School on Safety and Security Sciences, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest, Hungary
eleimat@gmail.com

Omar ALHARASEES
Department of Aeronautics and Naval Architecture, Faculty of Transportation Engineering and Vehicle Engineering. Budapest University of Technology and Economics, Budapest, Hungary
oalharasees@edu.bme.hu

Arnold OSZI
Doctoral School on Safety and Security Sciences, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest, Hungary
oszi.arnold@bgk.uni-obuda.hu

Abstract— **The aviation industry confronts escalating cyber threats jeopardizing operations and passenger safety, necessitating a shift towards human-centric airport cybersecurity. This study explores the integration of Artificial Intelligence (AI) in fortifying airport defenses and ensuring uninterrupted air travel. Deep learning algorithms and facial recognition systems enhance security by scrutinizing vast datasets and streamlining passenger authentication. Behavioral analytics detects anomalies indicative of security threats, while AI-driven cyber threat intelligence platforms facilitate proactive defense strategies. Blockchain and quantum encryption technologies promise enhanced resilience and security in aviation networks. The research conducts a comprehensive patent review using the Espacenet Patent Search engine to shed light on the latest innovations in airport cybersecurity. Our findings elucidate the pivotal role of technological advancements in safeguarding airports against evolving threats, contributing to the resilience of critical infrastructure.**

Keywords— Aviation security, Artificial Intelligence, deep learning algorithms, facial recognition, behavioral analytics.

I. INTRODUCTION

The aviation industry, a linchpin of global connectivity and economic prosperity, faces an escalating barrage of cyber threats jeopardizing operations and passenger safety [1]. In response, a paradigm shift towards human-centric airport cybersecurity has emerged, leveraging advanced technologies to fortify defenses and mitigate risks [2]. At the forefront of this evolution is the integration of Artificial Intelligence (AI) [3], offering innovative solutions to safeguard critical infrastructure and ensure uninterrupted air travel [4].

One pivotal application of AI in airport cybersecurity is the deployment of deep learning algorithms for real-time threat detection and anomaly analysis [5]. These algorithms are exemplified by systems developed to empower airports to scrutinize vast datasets from surveillance cameras and passenger screenings [6]. For instance, facial recognition systems enhance security by swiftly verifying passenger identities, and reducing wait times at checkpoints while bolstering defenses against potential threats [7].

Additionally, behavioral analytics has revolutionized the aviation sector's ability to detect and preempt insider threats and malicious activities. Leveraging AI-driven algorithms [8], platforms like those offered by Exabeam meticulously analyze user behavior patterns to identify deviations indicative of security breaches [9]. By monitoring employee access patterns and interactions with sensitive systems, airports can proactively mitigate risks posed by insider threats and unauthorized activities, ensuring the integrity of their operations.

Moreover, AI-powered training and awareness programs have reshaped cybersecurity education within the aviation industry, tailoring learning modules to individual needs and knowledge gaps [10]. CyberArk Security Awareness Training [11], for instance, employs AI algorithms to personalize training content for airport personnel. These programs enhance user awareness and readiness to combat evolving cybersecurity challenges by simulating real-world cyber threats and providing targeted guidance.

In parallel, the integration of AI-driven cyber threat intelligence platforms has bolstered airports' ability to anticipate and mitigate emerging risks [12]. Initiatives like the Aviation Information Sharing and Analysis Center (A-ISAC) facilitate collaborative information sharing and analysis among industry stakeholders [13]. By aggregating and analyzing threat data, these platforms empower airports to adopt proactive defense strategies and fortify their cybersecurity posture against evolving threats.

Looking ahead, transformative technologies such as blockchain and quantum encryption promise to enhance aviation networks' resilience and security [14], [15]. Blockchain technology, with its decentralized architecture and tamper-proof ledger, offers immutable records for aviation data and transactions [16]. Similarly, quantum encryption harnesses the principles of quantum mechanics to safeguard communications channels against interception

and tampering [17], [18], ensuring the integrity of sensitive information transmitted across aviation networks.

This research explores the multifaceted nature of human-centric airport security, highlighting the critical role of technological advancements in safeguarding airports against evolving threats. The technologies discussed, including deep learning algorithms, facial recognition systems, behavioral analytics, and others, offer a glimpse into the dynamic landscape of airport cybersecurity.

this article aims to provide a comprehensive overview of the technological trends shaping aviation and airport security developments. By delving into the integration of AI and other advanced technologies, the article explores innovative solutions aimed at fortifying defenses and mitigating risks in airport operations. Additionally, the article seeks to conduct a patent review of these technological trends using the Espacenet Patent search [19], shedding light on the latest innovations and developments in airport cybersecurity. Through this analysis, the article endeavors to offer valuable insights into the evolving landscape of aviation security and contribute to enhancing the resilience of critical infrastructure against cyber threats.

This study opted to primarily analyze patents related to airport security technologies for several reasons:

- Focus on Innovation: Patents offer a unique window into the latest technological inventions and advancements within the field. By examining patent applications, we gain insights into the direction of research and development efforts by various stakeholders in the aviation security sector.
- Timeliness: Patents are often filed before their corresponding academic publications, providing a glimpse into cutting-edge technologies that may not yet be fully explored in scholarly journals. This allows for the identification of emerging trends and potential future directions in airport security advancements.
- Complementary Data Source: Patent analysis serves as a valuable complement to research based on journal articles. It provides a broader perspective on technological innovation beyond just established academic research areas.

II. METHOD

In the method section, we explore the cutting-edge technological trends shaping human-centric airport security. The rapidly evolving field of aviation security relies heavily on technological advancements to safeguard airports against emerging threats. This section provides an overview of current technologies deployed in human-centric airport security, covering a range of innovations from biometric authentication to behavioral analytics. Each of these technologies plays a crucial role in enhancing threat detection, authentication processes, and overall security posture, thereby ensuring the safety and integrity of airport operations.

A. Evolution of Airport Security Technologies:

While patent data constitutes the primary focus of this study, it is essential to acknowledge the broader context of advancements in airport security technologies gleaned from recent academic literature. Research confirms deep learning algorithms effectively analyze X-ray scans and passenger behavior, enhancing airport security by detecting anomalies and suspicious activities [20], [21]. Ongoing improvements in facial and iris recognition systems expedite passenger processing while fortifying security against spoofing attacks [22]. The adoption of Cyber Threat Intelligence (CTI) platforms enables proactive identification and mitigation of cyber risks through collaborative information sharing [23]. Blockchain enhances airport operations' security and transparency by providing secure, immutable records for critical aviation data storage [24]. Quantum encryption ensures robust protection against cyber threats and espionage [25], strengthening airport security overall.
Autonomous security vehicles equipped with AI patrol perimeters, detecting anomalies and unauthorized access [26], thereby enhancing perimeter security [27]. Integrated biometric systems improve accuracy and reliability in passenger authentication, mitigating vulnerabilities [28]. Machine learning algorithms proactively identify emerging risks by analyzing diverse data sources and adapting security protocols accordingly [29]. Predictive analytics forecast threats and vulnerabilities, allowing prioritization of security resources to prevent breaches [30]. Information sharing among stakeholders enhances situational awareness and facilitates coordinated responses to security incidents, addressing challenges more effectively.

B. Emerging Trends in Airport Security Technologies:

- **Deep learning airport security**: Deep learning, a subset of machine learning, enables airports to analyze vast datasets for anomaly detection and threat prediction [31]. For instance, deep learning algorithms can process surveillance footage to identify suspicious behaviors or objects, enhancing security screening processes. Utilizing some specialized algorithms in deep learning-based facial recognition systems for airports, aiding in passenger authentication and security.
- **Facial recognition airport**: Facial recognition technology allows airports to streamline passenger authentication processes by verifying identities based on facial features [32]. For example, airports deploy facial recognition systems at check-in kiosks and boarding gates, reducing wait times and enhancing security.
- **Behavioral analytics aviation**: Behavioral analytics leverages machine learning to analyze user behavior patterns and detect anomalies indicative of security threats [33]. For airports, behavioral analytics can monitor employee access patterns, identifying unauthorized activities or insider threats.
- **Cyber threat intelligence airport**: Cyber threat intelligence involves collecting and analyzing information on potential cyber threats to anticipate and mitigate security risks [23]. In the aviation sector, organizations collaborate to share threat intelligence, enabling proactive defense measures.

- **Blockchain aviation security**: Blockchain technology offers secure and transparent data storage for critical aviation information, such as passenger records and flight data [34]. Blockchain enhances security and trust in aviation operations by decentralizing data storage and ensuring tamper-proof records [24]. Initiatives like Winding Tree explore blockchain applications in airline ticketing [35], reducing fraud and improving data integrity in the travel industry.
- **IoT airport cybersecurity**: The Internet of Things (IoT) introduces interconnected devices in airports, ranging from security cameras to baggage scanners, increasing the attack surface for cyber threats [36]. To address IoT security risks, airports deploy solutions like those from Palo Alto Networks [37], providing network segmentation and real-time threat detection capabilities. These measures protect against IoT-related vulnerabilities and ensure the integrity of airport operations.
- **Biometric authentication aviation**: Biometric authentication utilizes unique biological traits for identity verification, enhancing security in aviation processes like boarding and immigration [28]. Airports like Heathrow Airport implement biometric authentication systems, enabling passengers to undergo seamless identity verification using facial scans or fingerprints. This reduces queue times and enhances overall security at checkpoints.
- **Cloud security airport**: Cloud computing enables airports to store and process large volumes of data efficiently, but it also introduces security challenges. Cloud security solutions from providers offer encryption, access controls, and threat detection mechanisms to safeguard airport data and applications [38]. These measures ensure the confidentiality and integrity of sensitive information stored in the cloud.
- **Autonomous cybersecurity drones airport**: Autonomous drones equipped with sensors and AI algorithms patrol airport perimeters [39], detecting unauthorized drone incursions and potential security threats. Companies like Dedrone provide drone detection and mitigation solutions for airports [40], protecting against drone-related security breaches. These autonomous drones enhance situational awareness and response capabilities, bolstering airport security measures.
- **Quantum encryption aviation**: Quantum encryption employs principles of quantum mechanics to secure communication channels in aviation networks. By leveraging quantum key distribution (QKD) protocols [41], airports can achieve unparalleled levels of data security and privacy. Initiatives like the Quantum Communications Infrastructure project explore quantum encryption applications in aviation, safeguarding sensitive information from cyber threats and espionage.

In addition, the article outlines the approach for conducting a patent review to analyze the novel solutions and advancements within this domain. For conducting the patent review, the Espacenet Patent Search engine serves as the primary and sole source, providing comprehensive access to patents relevant to the technological trends outlined in this study.

III. RESULTS AND DISCUSSIONS

The results section presents the outcomes derived from our comprehensive analysis, emphasizing the findings obtained through the patent review process. This section elucidates the novel developments and advancements observed in airport cybersecurity technologies, contributing to the scholarly understanding of the evolving trends in this field.

The following table 1 presents an overview of the emerging trends in airport security technologies, highlighting the patent count for each category. This analysis encompasses a wide spectrum of technological innovations deployed in airport security, reflecting the current landscape of aviation security measures worldwide.

TABLE I. Patents Count of Emerging Airport Security Technologies [19].

Emerging Trends in Airport Security Technologies	Patents Count
Deep learning airport security	6497
Facial recognition airport	6913
Behavioral analytics aviation	4246
Cyber threat intelligence airport	1157
Blockchain aviation security	1329
IoT airport cybersecurity	2025
Biometric authentication aviation	4165
Cloud security airport	8016
Autonomous cybersecurity drone airport	1091
Quantum encryption aviation	873

As depicted in both Table 1 and Figure 1, deep learning algorithms, constituting 18% of the total patents reviewed, are instrumental in augmenting airport security through real-time threat detection and anomaly analysis. Facial recognition technology, accounting for 19% of the patents, streamlines passenger authentication processes while enhancing security measures at various checkpoints within airports.

Behavioral analytics in aviation, representing 12% of the patents, revolutionizes security protocols by leveraging machine learning to detect anomalies indicative of security threats. Similarly, cyber threat intelligence, blockchain aviation security, and IoT airport cybersecurity collectively contribute to fortifying airport defenses against evolving cyber threats, each comprising a notable percentage of the patents reviewed.

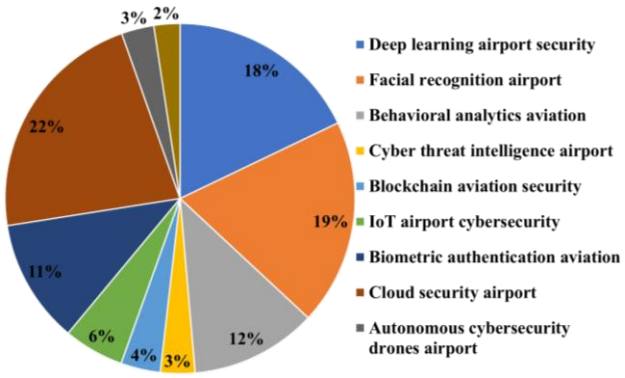

Figure 1. Distribution of Patents Across Emerging Airport Security Technologies.

Biometric authentication aviation, a category encompassing 11% of the patents, introduces robust identity verification measures, thereby enhancing security protocols during boarding and immigration processes. Cloud security solutions, constituting 22% of the patents, address the security challenges associated with cloud computing in airport operations, ensuring the confidentiality and integrity of sensitive data stored in cloud environments.

Autonomous cybersecurity drones, accounting for 3% of the patents, offer dynamic surveillance capabilities, patrolling airport perimeters to detect unauthorized drone incursions and potential security threats. Quantum encryption aviation, while representing a smaller percentage of the patents at 2%, underscores the significance of leveraging quantum mechanics to secure communication channels within aviation networks, safeguarding sensitive information from cyber threats and espionage.

This comprehensive analysis provides insights into the technological trends shaping airport security worldwide, emphasizing the critical role of innovation in enhancing the safety and integrity of airport operations amidst evolving security challenges.

IV. Conclusions

In conclusion, this study underscores the critical role of technological advancements in bolstering airport cybersecurity amidst escalating cyber threats. By integrating AI and other innovative solutions, airports can fortify defenses, enhance threat detection, and ensure the safety of operations and passengers. The deployment of deep learning algorithms, facial recognition systems, and behavioral analytics exemplifies the transformative potential of AI in augmenting security measures within airport environments.

Moreover, our comprehensive patent review reveals a diverse landscape of emerging technologies, ranging from biometric authentication to quantum encryption, each contributing to the resilience of airport security. The findings underscore the necessity for continuous innovation and proactive defense strategies to mitigate evolving cyber threats. By shedding light on the latest developments in airport cybersecurity, this research aims to inform policymakers, industry stakeholders, and researchers, facilitating the adoption of effective security measures and enhancing the resilience of critical infrastructure in the aviation sector.

In conclusion, as airports continue to navigate the complex landscape of cyber threats, embracing technological innovations and leveraging AI-driven solutions will be paramount in safeguarding against evolving risks and ensuring the integrity of airport operations in an increasingly digitized world.

References

[1] Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X., "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," *Inf. 2022, Vol. 13, Page 146*, vol. 13, no. 3, p. 146, Mar. 2022, doi: 10.3390/INFO13030146.

[2] M. Grobler, R. Gaire, and S. Nepal, "User, Usage and Usability: Redefining Human Centric Cyber Security," *Front. Big Data*, vol. 4, p. 583723, Mar. 2021, doi: 10.3389/FDATA.2021.583723/BIBTEX.

[3] O. Alharasees, O. H. Adali, and U. Kale, "Human Factors in the Age of Autonomous UAVs: Impact of Artificial Intelligence on Operator Performance and Safety," pp. 798–805, Jun. 2023, doi: 10.1109/ICUAS57906.2023.10156037.

[4] D. Ivanov, E. Pelipenko, A. Ershova, and A. Tick, "Artificial Intelligence in Aviation Industry," *Lect. Notes Data Eng. Commun. Technol.*, vol. 157, pp. 233–245, 2023, doi: 10.1007/978-3-031-24434-6_22/FIGURES/2.

[5] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports," *IEEE Access*, vol. 8, pp. 209802–209834, 2020, doi: 10.1109/ACCESS.2020.3036728.

[6] S. C. A. Thomopoulos, S. Daveas, and A. Danelakis, "Automated real-time risk assessment for airport passengers using a deep learning architecture," *https://doi.org/10.1117/12.2519857*, vol. 11018, pp. 212–223, May 2019, doi: 10.1117/12.2519857.

[7] R. Abeyratne, "Aviation and Cybersecurity in the Digital World," *Aviat. Digit. Age*, pp. 173–211, 2020, doi: 10.1007/978-3-030-48218-3_10.

[8] A. K. Jain, J. de Ruiter, I. Häring, M. Fehling-Kaschek, and A. Stolz, "Design, Simulation and Performance Evaluation of a Risk-Based Border Management System," *Sustain. 2023, Vol. 15, Page 12991*, vol. 15, no. 17, p. 12991, Aug. 2023, doi: 10.3390/SU151712991.

[9] "Behavioral Analytics - Exabeam." https://www.exabeam.com/feature/behavioral-analytics/ (accessed Mar. 16, 2024).

[10] M. Youseftorkaman, A. Kangaranifarahani, and D. Dana, "Applications of Artificial Intelligence in the Aviation Industry and Air Accidents," *Math. Stat. Eng. Appl.*, vol. 72, no. 2, pp. 178 – 192–178 – 192, Sep. 2023, Accessed: Mar. 16, 2024. [Online]. Available: https://www.philstat.org/index.php/MSEA/article/view/2832

[11] E. Carmel and E. M. Roche, "The dominant cybersecurity industry clusters: evolution and sustainment," *Ind. Innov.*, vol. 30, no. 3, pp. 361–391, Mar. 2023, doi: 10.1080/13662716.2022.2145938.

[12] F. Rodrigues, I. Kabashkin, B. Misnevs, and O. Zervina, "Artificial Intelligence in Aviation: New Professionals for New Technologies," *Appl. Sci. 2023, Vol. 13, Page 11660*, vol. 13, no. 21, p. 11660, Oct. 2023, doi: 10.3390/APP132111660.

[13] F. Lekota and M. Coetzee, "An aviation sector CSIRT for Sub-Saharan Africa," *Commun. Comput. Inf. Sci.*, vol. 1166 CCIS, pp. 28–42, 2020, doi: 10.1007/978-3-030-43276-8_3/FIGURES/4.

[14] J. Li, Z. Peng, A. Liu, L. He, and Y. Zhang, "Analysis and Future Challenge of Blockchain in Civil Aviation Application," *2020 IEEE 6th Int. Conf. Comput. Commun. ICCC 2020*, pp. 1742–1748, Dec. 2020, doi: 10.1109/ICCC51575.2020.9345297.

[15] X. Li, H. Zhao, and W. Deng, "BFOD: Blockchain-Based Privacy Protection and Security Sharing Scheme of Flight Operation Data," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3392–3401, Jan. 2024, doi: 10.1109/JIOT.2023.3296460.

[16] R. W. Ahmad, K. Salah, R. Jayaraman, H. R. Hasan, I. Yaqoob, and M. Omar, "The Role of Blockchain Technology in Aviation Industry," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 4–15, Mar. 2021, doi: 10.1109/MAES.2020.3043152.

[17] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini,

"Quantum Internet - Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 4, pp. 2218–2247, 2021, doi: 10.1109/COMST.2021.3109944.

[18] O. Alharasees, A. Jazzar, and U. Kale, "Misunderstandings in Aviation Communication," pp. 131–138, 2023, doi: 10.1007/978-3-031-32639-4_18.

[19] "Espacenet – patent search." https://worldwide.espacenet.com/patent/ (accessed Jun. 13, 2023).

[20] M. Memarzadeh, A. Akbari Asanjan, and B. Matthews, "Robust and Explainable Semi-Supervised Deep Learning Model for Anomaly Detection in Aviation," *Aerosp. 2022, Vol. 9, Page 437*, vol. 9, no. 8, p. 437, Aug. 2022, doi: 10.3390/AEROSPACE9080437.

[21] M. J. Bierrings, G. Sivakumar, N. Wunderlich, M. J. Bierrings, G. Sivakumar, and N. Wunderlich, "Blockchain in the Aviation Industry: A Decentralized Solution to the Transparency Issue in Baggage Handling," *Bus. Digit. Transform.*, pp. 45–72, 2024, doi: 10.1007/978-3-031-33665-2_3.

[22] A. Hattab and A. Behloul, "Face-Iris multimodal biometric recognition system based on deep learning," *Multimed. Tools Appl.*, vol. 83, no. 14, pp. 43349–43376, Apr. 2023, doi: 10.1007/S11042-023-17337-Y/TABLES/13.

[23] M. Klenka, "Aviation cyber security: legal aspects of cyber threats," *J. Transp. Secur.*, vol. 14, no. 3–4, pp. 177–195, Dec. 2021, doi: 10.1007/S12198-021-00232-8/METRICS.

[24] Karamitsos, I.; Papadaki, M.; Al-Hussaeni, K.; Kanavos, A., "Transforming Airport Security: Enhancing Efficiency through Blockchain Smart Contracts," *Electron. 2023, Vol. 12, Page 4492*, vol. 12, no. 21, p. 4492, Nov. 2023, doi: 10.3390/ELECTRONICS12214492.

[25] C. J. Pugh *et al.*, "Airborne demonstration of a quantum key distribution receiver payload," *Opt. InfoBase Conf. Pap.*, vol. Part F81-EQEC 2017, 2017, doi: 10.1109/CLEOE-EQEC.2017.8087396.

[26] V. Kharchenko, O. Illiashenko, H. Fesenko, and I. Babeshko, "AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis," *Commun. Comput. Inf. Sci.*, vol. 1689 CCIS, pp. 66–79, 2022, doi: 10.1007/978-3-031-20215-5_6/FIGURES/3.

[27] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends," *Intell. Serv. Robot. 2023 161*, vol. 16, no. 1, pp. 109–137, Jan. 2023, doi: 10.1007/S11370-022-00452-4.

[28] J. Horkay, S. Al-Rabeei, P. Korba, M. Hovanec, and V. Tymofiiv, "Opportunities for the Use of Biometric Technology in Air Transport," *EAI/Springer Innov. Commun. Comput.*, pp. 151–163, 2023, doi: 10.1007/978-3-031-28225-6_10/FIGURES/5.

[29] M. Yousefzadeh Aghdam, S. R. Kamel Tabbakh, S. J. Mahdavi Chabok, and M. Kheyrabadi, "Optimization of air traffic management efficiency based on deep learning enriched by the long short-term memory (LSTM) and extreme learning machine (ELM)," *J. Big Data*, vol. 8, no. 1, pp. 1–26, Dec. 2021, doi: 10.1186/S40537-021-00438-6/TABLES/8.

[30] M. Moll, T. Berg, S. Ewers, and M. Schmidt, "Predictive Analytics in Aviation Management: Passenger Arrival Prediction," pp. 667–674, 2020, doi: 10.1007/978-3-030-48439-2_81.

[31] R. Arun Kumaar, S. Malavika, S. Monisha, B. Sowmiya Bharani, and M. Devanathan, "A Review to Enhance Operations in an Airport with a Deep Learning and Computer Vision Approach," pp. 145–153, 2023, doi: 10.1007/978-981-19-3590-9_12.

[32] M. O. Oloyede, G. P. Hancke, and H. C. Myburgh, "A review on face recognition systems: recent approaches and challenges," *Multimed. Tools Appl.*, vol. 79, no. 37–38, pp. 27891–27922, Oct. 2020, doi: 10.1007/S11042-020-09261-2/TABLES/15.

[33] C. Zhang and Y. Zhang, "Psychological Mechanism of Civil Aviation Staff's Unsafe Behavior," *Commun. Comput. Inf. Sci.*, vol. 1581 CCIS, pp. 251–256, 2022, doi: 10.1007/978-3-031-06388-6_33/FIGURES/1.

[34] O. Alharasees, M. S. M. Abdalla, and U. Kale, "Digitalization in Aviation MRO Training," *2023 New Trends Aviat. Dev.*, pp. 10–14, Nov. 2023, doi: 10.1109/NTAD61230.2023.10380173.

[35] D. Pinto Lopes, P. Rita, and H. Treiblmaier, "The impact of blockchain on the aviation industry: Findings from a qualitative study," *Res. Transp. Bus. Manag.*, vol. 41, p. 100669, Dec. 2021, doi: 10.1016/J.RTBM.2021.100669.

[36] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing," *J. Supercomput.*, vol. 80, no. 3, pp. 3738–3816, Feb. 2024, doi: 10.1007/S11227-023-05616-2/TABLES/6.

[37] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "The SAir-IIoT Cyber Testbed as a Service: A Novel Cybertwins Architecture in IIoT-Based Smart Airports," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2368–2381, Feb. 2023, doi: 10.1109/TITS.2021.3106378.

[38] S. Anand and M. Dave, "Cybersecurity Resiliency for Airports as a Critical Infrastructure," *Lect. Notes Electr. Eng.*, vol. 1075 LNEE, pp. 1–16, 2024, doi: 10.1007/978-981-99-5091-1_1/TABLES/1.

[39] F. L. Chiper, A. Martian, C. Vladeanu, I. Marghescu, R. Craciunescu, and O. Fratu, "Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution," *Sensors 2022, Vol. 22, Page 1453*, vol. 22, no. 4, p. 1453, Feb. 2022, doi: 10.3390/S22041453.

[40] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors 2020, Vol. 20, Page 3537*, vol. 20, no. 12, p. 3537, Jun. 2020, doi: 10.3390/S20123537.

[41] A. Zaher, J. Rabaa, L. R. Kumar, and N. Rajesh Pandian, "Quantum Key Distribution for ADS-B Data Transmission Security in Aircraft," *2023 14th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2023*, 2023, doi: 10.1109/ICCCNT56998.2023.10307790.