Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience

Eugene Pik

College of Aviation, Embry-Riddle Aeronautical University

1 Aerospace Boulevard Daytona Beach, FL 32114 USA

December 1, 2023

Author Note

Eugene Pik pike@my.erau.edu https://orcid.org/0000-0001-6296-919X

Statements and Declarations

The authors have no relevant financial or non-financial interests to disclose.

Acknowledgements

The author would like to thank the Embry-Riddle Aeronautical University Worldwide Campus - Virtual Environment for Communication: Teaching, Outreach, and Research (**VECTOR**) and the College of Arts and Sciences (**COMPASS)** Research Mentoring Program for their support.

Abstract

This literature review article explores how artificial intelligence (AI) is revolutionizing airport security by automating threat analysis and identification processes. These advancements not only enhance security measures but also improve speed and accuracy. The capacity of AI to predict threats by analyzing vast passenger data helps identify potential risks. Balancing these breakthroughs are ethical and privacy concerns, stressing the importance of transparency and privacy protection to gain public trust. While AI systems' reliability and accuracy are central to balancing security and passenger convenience, the future of airport security depends on the effective integration of AI technologies. Biometrics and other transformative safety measures are discussed, with the suggestion for further research on optimizing real-time authentication systems, studying various AI strategies, and enhancing AI-based intrusion detection systems to prepare for future threats. The article is targeted towards AI, cybersecurity, and airport security professionals and researchers. Policymakers and decision-makers in the aviation and transportation sectors may also find value in understanding the impact of AI on airport security, ethical considerations, and future trends and research directions.

Keywords: AI biometric screening, AI threat detection, AI predictive threat analysis, AI passenger processing, AI security checks, AI airport security

1. Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience

The article provides a comprehensive review of the current state of AI in airport security. It covers a wide range of topics, from the practical applications of AI in threat detection and predictive threat analysis to the critical issues of accuracy, reliability, and data privacy. The balance between security and passenger convenience is also examined, alongside a detailed discussion on the ethical considerations of AI decision-making. Furthermore, the paper explores emerging AI technologies, their potential to transform global airport security standards, and future research and development areas. The goal of the article is to provide a nuanced understanding of the rapidly evolving landscape of AI in airport security, outlining the opportunities, challenges, and the path forward.

2. Method

The methodology of this article is centered on a literature review and analysis of the studies published on the use of AI in airport security. The literature review began by sourcing relevant academic papers, case studies, reports, and other scholarly works published on major databases, such as IEEE Xplore, ScienceDirect, Google Scholar, and SpringerLink. The keywords used in the search included but not limited to "AI airport security", "AI biometric screening", "AI threat detection", " airport security predictive analysis", " airport security Artificial Intelligence", "AI privacy concerns", "AI ethical considerations", “AI predictive threat analysis”, “AI passenger processing” and “AI security checks”.

A pool of studies was gathered based on these search criteria. The articles underwent a review, which included an examination of the research objectives, methodologies, findings, and conclusions. The selected studies underwent systematic analysis, focusing on their methodologies and the use of AI technologies. This included strategies for threat detection, predictive threat analysis, preemptive risk identification, and ethical and privacy concerns raised. This approach provided a comprehensive understanding of AI's current role in airport security, potential developments, challenges, and directions for future research.

3. Historical Perspective on the Use of AI in Airport Security.

In the realm of the aviation industry, airport security serves as a fundamental pillar that safeguards passengers, crew, and aircraft from harmful threats, criminal activities, and potential terrorist exploits. The core objective of security protocols is to prevent attempts at smuggling contraband, weapons, and explosives into airplanes, thereby decreasing the risk of hijackings or acts of terrorism. The process of formulating airport security measures is an integral factor that guides the design and construction of airport infrastructure (Maksymiuk et al., 2022). Over the course of air travel history, airport security technologies have experienced notable advancements. In the initial stages, security measures were minimal and primarily centered around hijacking prevention, however, as threats evolved, security technologies also underwent transformative developments.

Traditional airport security systems relied heavily on manual processes and human judgment, which were often time-consuming and susceptible to errors. The integration of AI has revolutionized airport security by automating various processes, thus improving efficiency and accuracy. The deployment of AI in the reconciliation process for passengers who are under suspicion of carrying dangerous and prohibited items plays a vital role (Raja & Sutarwati, 2023). The incorporation of AI-enhanced systems at Security Check Points (SCP) has led to significant progress in the detection and handling of dangerous goods. During busy travel times and times of heightened security alerts, AI helped in managing the workload and improving the performance of aviation security officers (Susanti & Frisnawati, 2023).

In the initial phase of incorporating AI into airport security, AI was primarily used for luggage screening. AI algorithms analyzed X-ray images of baggage to identify prohibited items like weapons and explosives. AI was also used for access control, validating identities of individuals entering the airport's secure zones. This was done using biometric systems, such as facial recognition or fingerprint scans. The implementation of Safety Management Systems (SMS) for heliport operational personnel is an example of how AI has been utilized in aviation security to ensure flight safety and security (Pratiwi & Prayudhista, 2023).

One of the early applications of AI in airport security was Network Intrusion Detection System (NIDS). AI algorithms were employed to analyze network traffic and detect any unauthorized or potentially harmful network activities. Chen et al. (2023) clarified how AI was used to optimize the data normalization process and combine the Principal Component Analysis (PCA) feature selection method to propose an optimized MaxAbs-DT classifier model for NIDS. AI outperformed other existing models in detecting network intrusions, validating the effectiveness of AI in enhancing security.

Another early application of AI in airport security was in the education and training of security personnel. AI was used to create simulations and training programs that helped security personnel to better understand and respond to various security threats. The role of AI in higher education, including the training of airport security personnel, was explained in a case study conducted at Georgia State University (Lainjo & Tsmouche, 2023). That case study demonstrated the benefits of AI adoption in higher education, which is also critical for training airport security personnel.

4. AI Technologies in Screening Processes and Threat Detection

4.1 Automated X-ray Scanning

Automated X-ray scanning is a non-invasive technology widely used in airport security to inspect the contents of luggage and carry-on bags. It employs X-rays to create images of the objects inside a bag or container without opening it. As X-rays pass through an object, dense materials such as metals absorb more X-rays and appear darker on the screen, while less dense materials appear lighter. This technology is crucial for quickly and efficiently identifying potential threats or prohibited items in luggage (Liang et al., 2018).

4.1.1 The Role of AI in Improving the Accuracy of X-ray Scanning

AI plays a significant role in enhancing the accuracy of X-ray scanning in airport security. By employing deep learning algorithms and neural networks, AI can analyze X-ray images in real-time and detect prohibited items or potential threats with higher precision than manual inspection. AI algorithms are trained on large datasets of X-ray images to recognize the characteristics of various objects, including weapons, explosives, and other contraband. This enables AI systems to make rapid and accurate decisions, reducing false positives and enhancing the efficiency of security screening processes (Petrozziello & Jordanov, 2019).

4.1.2 Case Studies of AI-enhanced X-ray Scanning.

In recent years, airports around the world have been integrating AI into their security systems to enhance X-ray scanning processes. A notable example is the Transportation Security Administration's (TSA) initiative to improve its Electronic Baggage Screening Program (EBSP) through AI (McKay et al., 2022). The iterative integration of AI and Machine Learning (ML) into the EBSP significantly improves the program's performance and efficiency over time. The integration of AI not only enhances safety but also improves cost-effectiveness and travel convenience for the public.

Another example of AI-enhanced X-ray scanning is the FORTIFIER framework, which is designed to detect suspicious artifacts in airports (Canizares et al., 2018). The framework combines multiple image detection algorithms, run in a distributed setting, with the goal of identifying a broad range of weapons such as firearms, blades, and explosives through the use of X-ray devices. The software is deployed in a cloud environment and is modeled using Finite State Machines (FSMs) for recognizing suspicious artifacts. The integration of AI algorithms into X-ray scanning systems enables the detection of a wide range of threatening objects with higher accuracy and efficiency.

4.2 Biometric Screening

Biometric screening is a security measure that uses an individual's unique physical characteristics, such as fingerprints, facial features, and iris patterns, to verify their identity. This technology is increasingly being adopted in airports to enhance security and streamline the passenger verification process. Biometric screening is considered more reliable than traditional methods such as ID cards or boarding passes, which can be lost or forged. In the context of airports, biometric screening is often integrated into automated border control systems and boarding gates, reducing the need for human intervention and thus increasing efficiency (Patel, 2018).

4.2.1 Facial Recognition and Fingerprint Scanning

AI plays a crucial role in enhancing the accuracy and efficiency of facial recognition and fingerprint scanning in biometric screening. In facial recognition, AI algorithms analyze facial features to create a mathematical representation, which is then compared with a database of known faces (Petrescu, 2019). Similarly, for fingerprint scanning, AI is used to analyze the ridges and valleys in a fingerprint and compare them against a database. Deep learning, a subset of AI, is particularly effective in improving the accuracy of biometric systems by enabling them to learn and improve from large datasets of biometric information (Prihodova & Hub, 2020).

4.2.2 Benefits of Biometric Screening in Airport Security

Biometric screening offers several benefits in airport security. It enhances security by providing a more accurate and reliable means of identity verification compared to traditional methods. Biometric screening streamlines the passenger processing experience, reducing queues and wait times, which is particularly beneficial in managing large volumes of passengers and improving the overall passenger experience. Additionally, biometric screening lessens the dependence on physical documents, which are susceptible to being lost or forged. In the context of health crises such as the COVID-19 pandemic, biometric screening can reduce physical contact and facilitate adherence to social distancing guidelines, contributing to a safer airport environment (Abdelwahed et al., 2020).

4.3 AI Algorithms for Detecting Prohibited Items in Luggage

AI algorithms have become an integral part of airport security systems, particularly in detecting prohibited items in luggage. Through the use of intelligent data analysis algorithms, such as deep learning, AI systems can analyze X-ray images of luggage to identify dangerous or prohibited objects. One of the challenges in using deep learning for this purpose is the scarcity of high-quality threat image data. In response to this, methods of detecting anomalies using regular data samples have demonstrated potential. For instance, Kolte et al. (2022) modified a Generative Adversarial Network (GAN) architecture known as Skip-GANomalyit by using a UNet++ style generator. The modified GAN architecture performed better in detecting dangerous objects in X-ray images. This approach is particularly beneficial in ensuring the security and safety of aviation by preventing passengers from carrying dangerous and prohibited goods.

4.4. Deep Learning and Neural Networks

Deep learning and neural networks are revolutionizing airport security by enhancing the ability to detect prohibited items and potential threats in luggage and on passengers. Convolutional Neural Networks (CNNs), a class of deep neural networks, are particularly effective in analyzing image data, such as X-ray and CT scans, used in airport security. Wang et al. (2020a) evaluated the possibility of extending automatic prohibited item detection from 2D X-ray imagery to volumetric 3D CT baggage security screening imagery using 3D CNN models. The findings indicate that 3D CNN models not only match the performance of conventional methods but also substantially reduce the time needed for inference.

4.5 Improving the Speed and Accuracy of Threat Detection

Enhancements in speed and precision of threat identification in airport security are vital for facilitating passenger flow while upholding strict security regulations. The utilization of Artificial Intelligence (AI) has proven to be instrumental in this aspect, with the ability to automate X-ray image analyses and promptly pinpoint potential threats. A study by Wang et al. (2020b) elaborates on a multi-object detection approach using a unified framework known as 3D RetinaNet. This approach, designed to recognize a variety of prohibited objects, exemplifies a feasible solution to this intricate problem.

The study also explores numerous strategies aimed at improving detection performance, including data augmentation and diversification of backbone networks. These innovative techniques underscore the adaptable nature of AI, which is key to enhancing threat detection accuracy and speed in airport security settings. By employing a model like the 3D RetinaNet, detection of different classes of objects can be achieved using a single model, making the security screening process more efficient. The research underscores the transformative potential of AI in redefining airport security and enhancing its effectiveness.

4.6 Predictive Threat Analysis

4.6.1 AI in Analyzing Passenger Data for Predictive Threat Analysis

Airport security is increasingly using AI to analyze passenger data for predictive threat analysis. By processing large volumes of data, AI algorithms can identify patterns and correlations that may indicate potential security threats. For instance, AI systems can analyze passenger booking data, travel history, and behavior patterns to assess the risk levels of individuals. This predictive analysis helps in identifying high-risk passengers and ensuring that security measures are taken proactively. In a study by Wei and Cheng (2022), AI was used to analyze various factors such as individual passenger demographic characteristics, travel purpose, and airport operation capacity to predict air passenger travel choices. The study concluded that due to the overcrowding at Beijing Capital International Airport, the primary strategy to consider is the diversion of passengers. This task will be jointly undertaken with Beijing Daxing International Airport and other nearby airports. This kind of predictive analysis can be extended to threat detection by analyzing data for potential security risks.

Hasan et al. (2023) demonstrated the use of AI in predicting cyber-security threats, which can be extrapolated to threat prediction in airport security. This research leverages machine learning to tackle Advanced Persistent Threat (APT) in cybersecurity. Utilizing various boosting algorithms, it predicts different APT types. By coupling these predictions with Explainable Artificial Intelligence (XAI), we can offer useful insights to the airport security stakeholders. This would help airport security teams not only detect potential threats but also understand the reasons behind these predictions, allowing for more effective response strategies.

4.6.2 Identifying Potential Security Risks before They Materialize

AI is increasingly being used in airport security to identify potential security risks before they materialize. This proactive approach, often referred to as predictive threat analysis, leverages AI algorithms to analyze passenger data and identify potential security risks. These algorithms can detect patterns and anomalies that might indicate a security threat, such as unusual travel patterns or suspicious behavior. This allows security personnel to intervene and take appropriate action before a potential threat becomes a real one. Zhao et al. (2020) developed an index system to classify airport passengers based on risk. The Back Propagation (BP) neural network classifier, enhanced by a Particle Swarm Optimization (PSO) algorithm, was trained, and tested with sample data. This system efficiently assesses passenger risk from five aspects: natural conditions, employment status, financial situation, creditworthiness, and flight details, with the aim of streamlining security procedures, reducing costs, and optimizing resource utilization.

5. The Accuracy and Reliability of AI Systems

In airport security, the accuracy and reliability of AI systems are paramount. AI systems are employed for various security measures including X-ray scanning, biometric screening, and threat detection. The accuracy of these systems determines how effectively they can identify threats or unauthorized items, while reliability ensures consistent performance over time. However, AI systems can sometimes produce false positives or fail to detect actual threats. Ensuring high accuracy and reliability requires continuous training of AI models with updated datasets, rigorous testing, and regular system evaluations. Risk modeling in distributed information systems poses various challenges. Palko et al. (2023) conducted an extensive analysis of risk assessment techniques and introduced an adaptable method for evaluating the risk of crucial information security incidents. This method employs a Decision Tree classification algorithm to dynamically analyze various factors in distributed information system metadata and metrics, enabling in-depth risk assessment for infrastructures of any scale.

The accuracy and reliability of AI systems, particularly in the context of detecting deception through facial cues and micro-expressions, is a subject of debate and concern. While AI systems were developed to enhance security, especially in high-risk areas such as airports, their effectiveness is questionable. One such system, iBorderCtrl is proposing the use of an Automatic Deception Detection System (ADDS), by analyzing a person's nonverbal micro expressions. The system aims to detect deception among travelers through nonverbal cues (Jupe & Keatley, 2020). However, while the concept of using micro-expressions as indicators of deception is intriguing, the psychological science supporting this theory is not yet firmly established. The cues that AI systems employ to detect deception often lack empirical backing and diagnostic value. These AI systems are frequently built upon a weak theoretical foundation and may struggle to accurately interpret the complexities and subtleties of human behavior. This situation raises significant concerns about the potential for false positives, which could have severe implications if these systems are relied upon in security contexts. Therefore, it is of utmost importance that these systems undergo rigorous testing and validation before they can be deemed reliable and accurate for practical use (Yan et al., 2013).

6. Ethical and Privacy Concerns, Balance of Security and Convenience

6.1 Ethical Considerations and Privacy Concerns

Ethical considerations and privacy concerns are paramount when it comes to the implementation of AI in airport security. The use of AI technologies such as facial recognition, biometric screening, and data analysis can significantly enhance security measures. However, it is essential to ensure that these technologies do not infringe upon individuals' privacy rights or lead to discrimination. For instance, data collected through AI systems must be handled with utmost confidentiality, and individuals should be informed about the kind of data being collected and how it will be used. AI systems should be transparent and accountable, ensuring that they do not exhibit biases that could lead to unfair treatment of certain groups of people. It is also crucial to have a human-centered approach that prioritizes the needs and values of individuals while employing AI technologies in airport security (Huriye, 2023).

Hagendorff (2020) describes that AI ethics is facing challenges due to lack of enforcement mechanisms and being used as a marketing strategy. Software requirement managers often overlook ethical implications due to distributed responsibility and lack of understanding of long-term societal consequences. There are efforts to address specific ethical issues, but many are not adequately addressed. To bridge the gap between AI ethics and technology, there is a need for a shift from checkbox guidelines to a more situation-sensitive ethical approach that emphasizes virtues, knowledge expansion, and responsible autonomy. This approach should integrate technical details with social and personality-related aspects.

6.2 Privacy Concerns and Data Protection

Privacy concerns and data protection are significant issues in airport security, especially with the integration of AI systems. AI systems often require access to personal data, such as biometric information, travel history, and identification documents. While this data is essential for security screening, there is a risk of misuse or unauthorized access. Data protection laws and regulations are crucial to ensure that personal data is handled securely, and that privacy is maintained. Passengers should be informed about the data being collected and how it is used.

Smart airports utilize technologies such as IoT, AI, Virtual Reality, Biometrics, and Cloud Computing to enhance operational efficiency and passenger experience. Alabsi and Gill (2021) reviewed the need to address passengers' digital information privacy concerns in smart airports through the Customer Journey Map (CJM) and Concerns for Information Privacy (CFIP) frameworks. Passengers' privacy challenges were identified and grouped into collection, errors, unauthorized use, and improper access. The findings suggest the necessity to address these concerns by implementing contemporary solutions that improve the privacy level of passengers' digital information. This includes identifying and categorizing challenges related to data collection, errors, unauthorized use, and improper access, and mapping them to current solutions while adhering to relevant standards and policies.

6.3 The Balance between Security and Passenger Convenience

Balancing security and passenger convenience is a challenging aspect of airport security. While stringent security measures are necessary to ensure the safety of passengers and aircraft, they can also lead to longer waiting times and a less pleasant travel experience. Wei and Cheng (2022) concluded that the most important factor when choosing an airport is its operational efficiency, particularly the speed of the security screening process. AI systems can help strike a balance by streamlining security processes, such as automated document verification and faster threat detection, which can reduce waiting times without compromising security. However, it is essential to ensure that these systems are transparent and do not infringe on passengers' rights or privacy.

7. Future Prospects and Trends

7.1 Emerging AI Technologies in Airport Security

Emerging AI technologies are playing a pivotal role in enhancing airport security. One such technology is biometric-based identity authentication, which includes Photoplethysmography (PPG) (Sarkar et al., 2016). PPG is gaining momentum due to its effectiveness and ease of implementation. A cloud-based system collects PPG signals from individuals through distributed sensors and communicates them to the cloud for authentication. The cloud server runs sophisticated algorithms to verify the identity and encrypts the signal for privacy. This is particularly useful in crowded places like airports to manage large signal traffic efficiently (Abdelaziz et al., 2023). Additionally, Information and Communication Technologies (ICT) and Multi Agent Systems (MAS) are being utilized to monitor various areas within airports, including terminals, car parks, and passenger facilities. These technologies contribute to improving safety and security by optimizing airport operations (Sahic & Cinac, 2022).

7.2 The Potential of AI in Transforming Global Airport Security Standards

AI technologies integrated with Wireless Sensor Networks (WSNs) have the potential to revolutionize global airport security standards by addressing security, fault detection, and Quality of Service (QoS) concerns (Osamy et al., 2022). These AI methodologies offer insights for tackling existing WSN difficulties and contribute to an enhanced understanding of current AI applications in security and QoS. For instance, AI can improve the security of WSNs by identifying and classifying threats more comprehensively, while optimizing sensor placement to enhance the QoS of WSNs. Furthermore, AI's ability to detect new cyber-attacks faster than humans makes it an indispensable component in constructing better protection against cybercrime in airport systems (Dash et al., 2022).

7.3 Future Challenges and Areas for Research and Development

While AI technologies are transforming airport security, there are challenges and areas that require further research and development. One of the challenges is ensuring the high fidelity and computational efficiency of biometric authentication systems like PPG in real-time environments such as airports (Abdelaziz et al., 2023). Additionally, there is a need for comprehensive studies and analyses of various AI schemes utilized in WSNs to recognize the most widely used techniques and the merits of employing various AI solutions to tackle airport security-related challenges (Osamy et al., 2022). The adoption of AI algorithms by companies should be encouraged to implement cybersecurity safeguards actively. This approach will enable businesses and consumers to realize that the most effective defense against cybercrime lies in leveraging AI technology. Future research could focus on assessing the study's utility by gathering extensive datasets with multiple dimensions of security features in IoT security services (Dash et al., 2022).

8. Conclusion

The integration of AI in airport security has proven to be a game-changer in enhancing the safety and efficiency of air travel. From automated X-ray scanning and biometric screening to predictive threat analysis, AI technologies have revolutionized the way airport security operates. The use of AI algorithms has significantly improved the accuracy of threat detection, reduced human error, and streamlined passenger processing. AI's ability to analyze large volumes of data and identify patterns has enabled proactive security measures, allowing potential threats to be identified and addressed before they materialize.

The implementation of AI in airport security is not without its challenges. Ethical considerations and privacy concerns are paramount, particularly with the use of biometric screening and data analysis. It is crucial to ensure that AI systems are transparent, accountable, and do not infringe upon individuals' privacy rights. Furthermore, the accuracy and reliability of AI systems are critical, requiring continuous training, rigorous testing, and regular system evaluations. Despite these challenges, the future of AI in airport security looks promising, with emerging technologies such as PPG and MAS offering new avenues for enhancing security measures. As AI continues to evolve, it holds the potential to transform global airport security standards and contribute to a safer and more efficient travel experience.

Looking ahead, the future of airport security lies in the continuous innovation and development of AI technologies. As security threats evolve, so must the technologies used to combat them. This requires ongoing research, development, and collaboration among stakeholders, including governments, airport authorities, technology providers, and passengers. By doing so, airport security can stay ahead of the curve, ensuring not only the safety and security of air travel but also a more seamless and positive experience for passengers worldwide.

Declarations

Ethical Approval

Not applicable

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Availability of data and materials

Not applicable

References

Abdelaziz, A. B., Rahimi, M. A., Alrabeiah, M. R., Ibrahim, A. B., Almaiman, A. S., Ragheb, A. M., & Alshebeili, S. A. (2023). Photoplethysmography data reduction using truncated singular value decomposition and Internet of Things computing. *Electronics*, *12*(1), Article 1. https://doi.org/10.3390/electronics12010220

Abdelwahed, H. J., Hashim, A. T., & Hasan, A. M. (2020). Segmentation approach for a noisy iris images based on hybrid techniques. *Engineering and Technology Journal*, *38*(11A), 1684–1691. https://doi.org/10.30684/etj.v38i11A.450

Alabsi, M. I., & Gill, A. Q. (2021). A review of passenger digital information privacy concerns in smart airports. *IEEE Access*, *9*, 33769–33781. https://doi.org/10.1109/ACCESS.2021.3061425

Canizares, P. C., Merayo, M. G., & Núñez, A. (2018). FORTIFIER: A FORmal disTrIbuted framework to improve the dEtection of thReatening objects in baggage. *Journal of Information and Telecommunication*, *2*(1), 2–18. https://doi.org/10.1080/24751839.2017.1347766

Chen, D., Song, Q., Zhang, Y., Li, L., & Yang, Z. (2023). Identification of network traffic intrusion using decision tree. *Journal of Sensors*, *2023*, e5997304. https://doi.org/10.1155/2023/5997304

Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: A review. *International Journal of Software Engineering & Applications*, *13*(5), 13–21. https://doi.org/10.5121/ijsea.2022.13502

Hagendorff, T. (2020). The ethics of AI ethics: An evaluation of guidelines. *Minds and Machines*, *30*(1), 99–120. https://doi.org/10.1007/s11023-020-09517-8

Hasan, Md. M., Islam, M. U., & Uddin, J. (2023). Advanced persistent threat identification with boosting and explainable AI. *SN Computer Science*, *4*(3), 271. https://doi.org/10.1007/s42979-023-01744-x

Huriye, A. Z. (2023). The ethics of artificial intelligence: Examining the ethical considerations surrounding the development and use of AI. *American Journal of Technology*, *2*(1), Article 1. https://doi.org/10.58425/ajt.v2i1.142

Jupe, L. M., & Keatley, D. A. (2020). Airport artificial intelligence can detect deception: Or am I lying? *Security Journal*, *33*(4), 622–635. https://doi.org/10.1057/s41284-019-00204-7

Kolte, S., Bhowmik, N., & Dhiraj. (2022). Threat object-based anomaly detection in X-ray images using GAN-based ensembles. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-022-08029-z

Lainjo, B., & Tsmouche, H. (2023). The impact of artificial intelligence on higher learning institutions. *International Journal of Education, Teaching, and Social Sciences*, *3*(2), Article 2. https://doi.org/10.47747/ijets.v3i2.1028

Liang, K. J., Heilmann, G., Gregory, C., Diallo, S. O., Carlson, D., Spell, G. P., Sigman, J. B., Roe, K., & Carin, L. (2018). Automatic threat recognition of prohibited items at aviation checkpoint with x-ray imaging: A deep learning approach. *Anomaly Detection and Imaging with X-Rays (ADIX) III*, *10632*, 1063203. https://doi.org/10.1117/12.2309484

Maksymiuk, Y., Chulinda, L., Korchova, H., & Pochka, K. (2022). Priority directions of international airport infrastructure development. *Strength of Materials and Theory of Structures*, *109*, Article 109. https://doi.org/10.32347/2410-2547.2022.109.301-316

McKay, S., Hartnett, G. S., & Held, B. (2022). *Airline security through Artificial Intelligence: How the transportation security administration can use machine learning to improve the electronic baggage screening program*. RAND Corporation. https://doi.org/10.7249/PEA731-1

Osamy, W., Khedr, A. M., Salim, A., El-Sawy, A. A., Alreshoodi, M., & Alsukayti, I. (2022). Recent advances and future prospects of using AI solutions for security, fault tolerance, and QoS challenges in WSNs. *Electronics*, *11*(24), Article 24. https://doi.org/10.3390/electronics11244122

Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. *Applied Sciences*, *13*(4), Article 4. https://doi.org/10.3390/app13042393

Patel, V. (2018). *Airport passenger processing technology: A biometric airport journey*. https://commons.erau.edu/edt/385

Petrescu, R. V. (2019). *Face recognition as a biometric application* (SSRN Scholarly Paper No. 3417325). https://doi.org/10.2139/ssrn.3417325

Petrozziello, A., & Jordanov, I. (2019). Automated deep learning for threat detection in luggage from X-Ray images. In I. Kotsireas, P. Pardalos, K. E. Parsopoulos, D. Souravlias, & A. Tsokas (Eds.), *Analysis of Experimental Algorithms* (pp. 505–512). Springer International Publishing. https://doi.org/10.1007/978-3-030-34029-2_32

Pratiwi, I. D. A., & Prayudhista, E. (2023). Implementation of Safety Management System (SMS) for heliport operational personnel at PT. Whitesky Aviation. *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia, 2*(1), Article 1. https://doi.org/10.57235/aurelia.v2i1.271

Prihodova, K., & Hub, M. (2020). Hand-based biometric system using convolutional neural networks. *Acta Informatica Pragensia*, *9*(1), 48–57. https://doi.org/10.18267/j.aip.131

Raja, M. F., & Sutarwati, S. (2023). Reconciliation analysis of passengers suspected of carrying dangerous and prohibited goods at Komodo Labuan Bajo airport security checkpoint. *QISTINA: Jurnal Multidisiplin Indonesia*, *2*(1), Article 1. https://doi.org/10.57235/qistina.v2i1.495

Sahic, A., & Cinac, D. (2022). Application of ICT as a key element for airport safety and security operations. *Science, Engineering and Technology*, *2*(2), Article 2. https://doi.org/10.54327/set2022/v2.i2.44

Sarkar, A., Abbott, A. L., & Doerzaph, Z. (2016). Biometric authentication using photoplethysmography signals. *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 1–7. https://doi.org/10.1109/BTAS.2016.7791193

Wang, Q., Bhowmik, N., & Breckon, T. P. (2020a). Multi-class 3D object detection within volumetric 3D computed tomography baggage security screening imagery. *2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 13–18. https://doi.org/10.1109/ICMLA51294.2020.00012

Wang, Q., Bhowmik, N., & Breckon, T. P. (2020b). On the evaluation of prohibited item classification and detection in volumetric 3D computed tomography baggage security screening imagery. *2020 International Joint Conference on Neural Networks (IJCNN)*, 1–8. https://doi.org/10.1109/IJCNN48605.2020.9207389

Wei, W., & Cheng, W. (2022). Design of air passenger travel choice intention prediction system based on deep learning. *Scientific Programming*, *2022*, e7340552. https://doi.org/10.1155/2022/7340552

Yan, W.-J., Wu, Q., Liang, J., Chen, Y.-H., & Fu, X. (2013). How fast are the leaked facial expressions: The duration of micro-expressions. *Journal of Nonverbal Behavior*, *37*(4), 217–230. https://doi.org/10.1007/s10919-013-0159-8

Zhao, Z., Zhang, C., & Guo, D. (2020). Analysis of risk-based airport passenger classification with PSO-BP neural network. *2020 39th Chinese Control Conference (CCC)*, 7344–7349. https://doi.org/10.23919/CCC50068.2020.9188750