Journal of Airline Operations and Aviation Management

Article

How Smart Airport is Paving the way for a Smart Access Concept: Technology's Role in the Digital Ecosystem of the Access Control Process

Sersinho Gardt[1], Catya Zuniga Alcaraz[2], Rob Satink[3]

[1]Researcher Aviation Security & Technology, Amsterdam University of Applied Sciences, The Netherlands

Email: s.r.gardt@hva.nl, Orcid id: https://orcid.org/0009-0006-9287-7089

[2]Associate Professor, Faculty of Technology – Aviation Academy, Amsterdam University of Applied Sciences, The Netherlands

Email: c.a.zuniga@hva.nl, Orcid id: https://orcid.org/0009-0004-2327-1337

[3]Independent consultant, The Netherlands

Email: rob@satinks.nl

DOI: https://doi.org/10.69978/jaoam.V3.I2.4

Abstract.

Airports have undergone a significant digital evolution over the past decades, enhancing efficiency, effectiveness, and user-friendliness through various technological advancements. Initially, airports deployed basic IT solutions as support tools, but with the increasing integration of digital systems, understanding the detailed digital ecosystem behind airports has become crucial. This research aims to classify technological maturity in airports, using the access control process as an example to demonstrate the benefits of the proposed taxonomy. The study highlights the current digital ecosystem and its future trends and challenges, emphasizing the importance of distinguishing between different levels of technological maturity. The role of biometric technology in security access control is examined, highlighting the importance of proper identification and classification. Future research could explore data collection, privacy, and cybersecurity impacts, particularly regarding biometric technologies in Smart Access Level 4.0. The transition from Smart Access Level 3.0 to 4.0 involves process automation and the introduction of AI, offering opportunities to increase efficiency and improve detection capabilities through advanced data analytics. The study underscores the need for global legislative frameworks to regulate and support these technological advancements.

Keywords: Biometric Technology, Digital Ecosystem, Process Automation, Smart Access, Smart Airport, Security Process.

Received 24 July 2024
Revised 10 October 2024
Accepted 15 October 2024

1. Introduction

Airports have been going through a digital evolution for the past decades. Every piece of technology used at an airport has made processes more efficient, effective, and people-friendly. In the early years of the digital evolution airports deployed basic IT solutions as support tools for the human (user, clients), however, with the increasing integration of digital systems at airports, it is important to understand in detail the digital ecosystem behind airports. For this, a proper classification of technological maturity in airports is presented, together with this, and as an example, the Access control process is presented and used to show the benefits of the proposed taxonomy. Also highlighted is the currently available digital ecosystem along with its future trends and challenges. This research aims to show the importance of the difference between airports' technological maturity levels. It is expected to propose a clear taxonomy to measure the technological maturity levels of different processes offered.

2. What is a Smart Airport?

The Smart Airport concept lacks a universally standardized definition within the aviation sector. It originated from advancements in the Internet of Things (IoT) and the Industry 4.0 revolution, as well as the need to address various challenges. IoT refers to technologies that connect everyday objects to the internet, facilitating new business models through digital transformation. With the rise of the 4th industrial revolution, manual operations are being replaced by automation, giving rise to smart airports, real-time data sharing, and e-enabled aircraft.

Smart airports are made possible through the integration of Connected Technologies (CT) across the entire ecosystem. These technologies include IoT, sensors, GPS, surveillance cameras, mobile phones, augmented reality devices, and AI algorithms that serve as decision support tools. Together, they optimize airport and aircraft operations. CT can collect a wide range of data, such as passenger credentials (e.g., through facial recognition) and track passenger behavior throughout the terminal, as well as sensitive air traffic communications. This creates vast amounts of data, often referred to as big data, which is typically managed and stored using cloud technologies [1].

Rubio-Andrada, Celemín-Pedroche, Escat-Cortés, and Jiménez-Crisóstomo [2] define smart airports as those designed to provide safe and efficient travel experiences, a need that became even more critical during the COVID-19 pandemic. Qi and Zhu [3] describe smart airports as a fusion of efficient self-service processes powered by IoT for offline operations, new information platforms for online operations, and advanced evaluation systems driven by big data. Similarly, Grodi, Rawat, and Rios-Gutierrez [4] define smart airports as those leveraging emerging technologies such as IoT, big data, and mobile applications to optimize infrastructure utilization and enhance the passenger experience. Nau and Benoit [5] suggest that smart airports are characterized by their ability to fully exploit technological advancements while aligning with strategic priorities, acknowledging the airport's unique context and constraints.

In our view, a "Smart Airport" refers to a technologically advanced aviation facility that integrates cutting-edge information and communication technologies to improve operational efficiency, elevate the passenger experience, and enhance overall safety and security. Smart airports leverage data-driven insights, the Internet of Things (IoT),

automation, and performance-based management to optimize various processes, such as "smart check-in," "smart security," "deep turnaround," and automated handling systems. These innovations streamline airport operations and offer a seamless, efficient journey for both passengers and stakeholders.

To further refine the Smart Airports concept, it is proposed to classify smart airports based on the maturity level of technology adoption in key areas. This approach allows for a structured understanding of how technology is integrated into various components of airport operations. By evaluating the maturity of digitalization, automation, and management, airports can build automated, flexible processes that align with business objectives. Rajapaksha and Jayasuriya [6] underscore the importance of technology adaptation as a marker for an airport's evolution from a digital maturity perspective. This work adopts a detailed taxonomy, as introduced by Teichert [7], to categorize airports according to their maturity levels in specific areas:

Digital Vision: Involves the governance, management, and execution of a digital strategy. It encompasses defining the business model, creating an IT roadmap to achieve the digital vision, and establishing organizational structures and practices that support digital business operations.

Digital Ecosystem: Focuses on digital transformation efforts to enhance IT infrastructure, promote cultural integration, and foster interconnected systems over isolated ones. Automation of operations and processes is emphasized to boost efficiency.

Digital Skills and Expertise: Highlights the importance of an agile and adaptable workforce with the necessary skills to support the development and implementation of digital initiatives. Leadership aligned with the digital vision and strategy is critical to successfully navigating digital transformation.

Customer Insight & Experience: Stresses the importance of understanding customer needs and preferences to provide personalized services and products. By leveraging customer behaviour insights, airports can align their processes to exceed expectations and deliver a superior passenger experience.

This taxonomy provides a structured framework for assessing the digital maturity of airports, helping them strategically advance their smart airport capabilities. By understanding the different levels of digital maturity, airports can make informed decisions on how to progress toward a fully realized smart airport model. Building upon the framework, we propose an enhancement to Rajapaksha's taxonomy, with a clear progression of digital maturity from basic manual operations to advanced, interconnected, and automated systems:

Airport 1.0: This is the foundational level, where airports offer only basic customer services, and most processes are manual. There is a significant lack of digital vision, and IT infrastructure is limited, with minimal implementation capabilities. While testing solutions and web information pages may exist, the use of software and IT solutions is scattered across a few stages of the passenger journey. A critical characteristic of this level is the absence of Self-Service

Technology (SST), which refers to the automated systems that allow passengers to perform tasks independently, without the need for direct staff assistance. As such, both the digital vision and ecosystem are practically non-existent.

Airport 2.0: At this stage, airports begin adopting Self-Service Technology (SST) alongside systems like Common Use Terminal Equipment (CUTE) and Common Use Passenger Processing Systems (CUPPS). Digital ecosystems start to take form, enabling the introduction of basic IT solutions such as Wi-Fi and standalone check-in kiosks. This early adoption of a digital ecosystem signals the emergence of digital skills among staff and passengers, creating a foundation for a more mature digital vision. However, these technologies remain in silos, and the system lacks full interconnection.

Airport 3.0: Airports at this level have achieved a more mature digital ecosystem. There is a robust interconnection between stakeholders and users, facilitating real-time sharing of information across different systems. The airport's digital vision incorporates customer insights, using them to drive new solutions. Additionally, advanced IT solutions and self-service facilities, such as automated bag drop and biometric check-ins, are widely integrated into daily operations. The digital skills of both passengers and staff are well-developed, contributing to smoother and more efficient processes.

Airport 4.0: The most advanced stage of airport digitalization, where the digital ecosystem is fully mature and operational. Airports at this level leverage real-time data sharing and automated systems to manage performance-based operations. Advanced algorithms and AI-driven decision-making tools optimize airport functions, enhancing efficiency and flexibility. The digital vision is fully realized, and the airport's organizational structure actively supports digital business practices. These airports continuously update their digital ecosystems to stay ahead of technological advancements, maintaining a proactive approach to innovation.

By enhancing Rajapaksha's taxonomy with this detailed progression, airports can assess their current digital maturity and identify the necessary steps to advance through the levels. This approach offers a clear roadmap for evolving from basic manual operations to fully integrated smart airports, aligning their digital vision with both business objectives and passenger needs. The taxonomy of Smart Airports provides a framework for analysing processes, concepts, and technologies at each level. It allows airports to define roadmaps for upgrading from one maturity level to the next by evaluating the readiness of specific solutions and processes that are in place.

3. The Access Control Process

Smart Access also addressed as Smart Security, similar to the Smart Airport concept, is a new concept born due to the IoT, the Industry 4.0 revolution, but also triggers the need for enhancing passengers' experience. In this context, Smart Access is about using intelligent technology for access control at restricted areas of airports. To get a better understanding of what Smart Access entails, it will have to clearly define the purpose of Access Control, its participants, the technology associated, etc.

The Access control process also addressed as the Security control process aims to provide measures put in place to prevent unauthorized entry of persons, vehicles, or both to an airport's restricted area or Security Restricted Area (SRA).

SRA is the airport space that is deemed a risk area and requires security control measures in addition to access control measures. Such measures include risk assessments, identification systems, checkpoints, background checks, screening, and security controls. Screening and security control are meant to "identify weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference" and prevent these from being introduced to SRA [8, 9]

Figure 1 presents each process describing the activities and tools used in the Access Control process. It should be noted that access control employs two main security control measures: valid documentation to allow access and, screening the users and their belongings to be free of threats. It also has to be highlighted that in the Airport taxonomy presented above, historically, the Access Control process has relied more on human interaction (security agents) to perform the access control process which positions this process in Airport 1.0 Level; however, nowadays it is becoming common that the passenger can have access to the airport secure areas by using automated machines & digital information to perform the required checks.

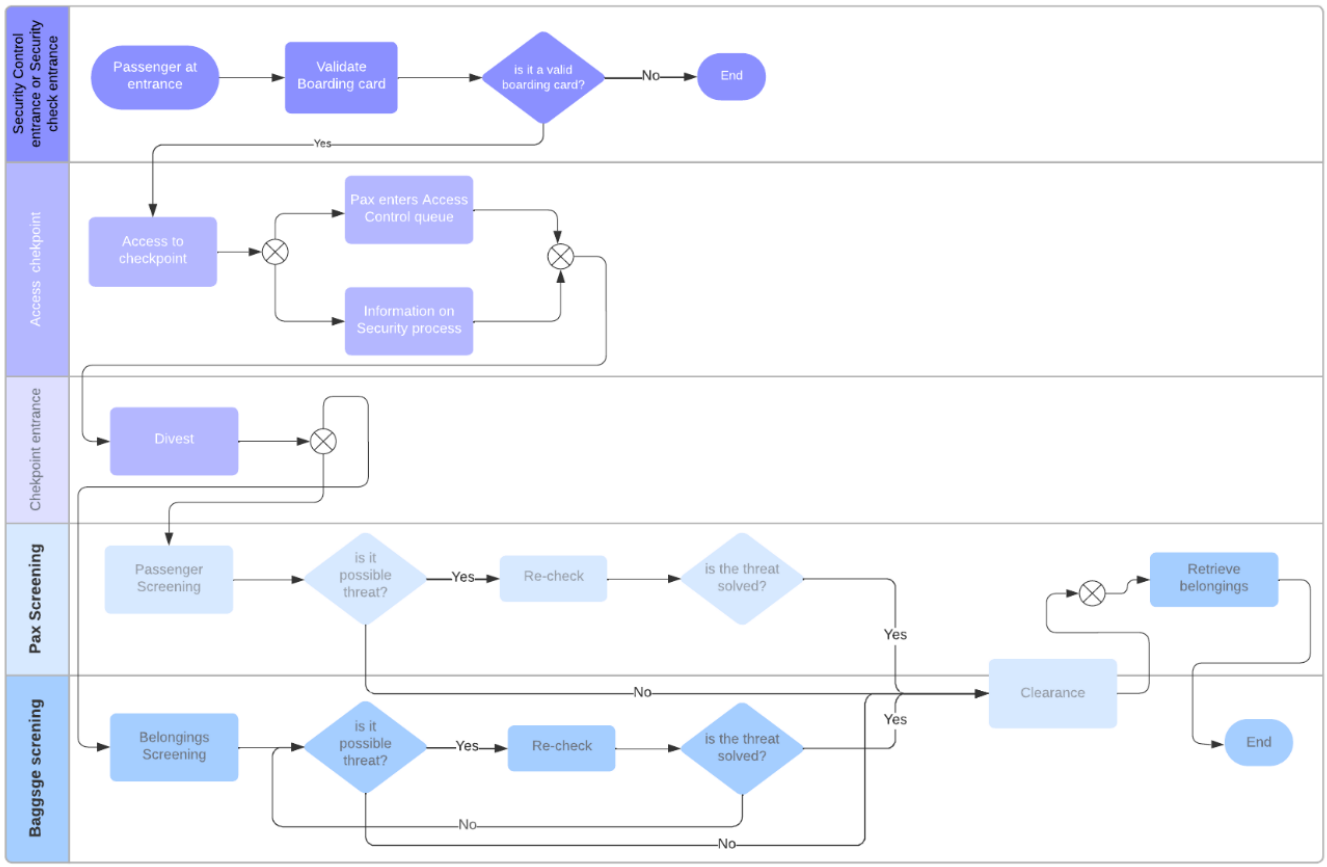

Figure 1. Access control process diagram

Unlike passengers, staff is sometimes allowed to carry certain prohibited items with them into airside. The usage of a badge by staff members is limited only to legitimate reasons to be in a specific area, such as work-related activities, and once a background check and training have been completed without any objections. This in turn allows managers to distinguish who can access the airside with what.

The Security Control entrance process starts at the so-called Security Control Areas which is the entrance to the Access Control facilities. To allow users (e.g., passengers or staff) access to the SRA, valid documentation is required. It should be noted that the Access Control process is similar for passengers and staff with some key variations since staff members have a higher recurrence of using the access control process, and therefore, different access control systems can be placed. For passengers, the Access Control technology has been quickly transitioning into the so-called "Self-service technology" triggering the Smart Access process into the secure area which means the transition from manual access control performed by an agent using basic tools for identifying threats, to an automated activity where digital boarding passes together with digital card reader allows the user the entrance to the SRA, see Table 1 for more details about the available technology.

Once the user has entered the Control area, the user queues to reach the Access Checkpoint where the user and his belongings are going to be scanned for security purposes. The user will walk towards the checkpoint encountering the security control queue. In most airports, the queuing time and area are used to provide information on the security process they will be subjected to, such that they are reminded of the screening steps and the experience is friendlier and more efficient. Some airports nowadays account with sensors and cameras which allow real-time management of passengers' flow which will trigger the transition from Airport 2.0 level to Airport 3.0 level.

After reaching the Access Checkpoint, users head towards a security lane by a service agent or an automated machine where the user has to divest. The divest process consists of removing items from the person and their belongings and placing them on a tray to be scanned. This process has also been transformed through time, moving to multiple-individual divesting stations with conveyors and trays to feed the screening process. This is supported by security agents that help users understand the scanning process and the items prohibited from entering SRA, this includes liquids, gels, sharp objects, and other potentially restricted items of various quantities and sizes.

Once the passenger has divested their belongings, the passenger is ready to move to the scanning process itself where both the passenger and their belongings are to be checked. Nowadays, the scanning for both, the user and their belongings in most of the airports is performed by security agents utilizing devices that are equipped with threat detection algorithms to further enhance security. The passenger walks through the metal detector or body scanner following any instructions provided by security personnel. The passengers' items placed in trays are moved through a conveyor system for screening. This scan is meant to identify any prohibited items in carry-on baggage, hence in case of an anomaly, on the passenger or its belongings, a manual search will take place.

After passing through the metal detector or body scanner without suspicion of a threat, the user is cleared to continue collecting their belongings from the trays as they come through the scanning machine. Finally, when the passenger retrieves all its belongings, the passenger will continue their journey through the airport.

4. Emerging technology in security access control

The evolution of airport security technology has been driven by the dual objectives of enhancing operational efficiency and safety, while also improving the passenger experience. In the early days of commercial aviation, security measures were rudimentary [10]. Airports primarily relied on simple screening methods, such as visual checks of tickets and personal identification. The focus was on verifying passengers' tickets rather than preventing security threats. However, the 1970s brought a pivotal shift in airport security with the introduction of metal detectors and X-ray machines for baggage screening. This advancement was driven by the rise in hijacking incidents and emerging security threats. Metal detectors enabled security personnel to detect weapons or other metallic objects on passengers, while X-ray machines allowed for detailed inspection of carry-on luggage for prohibited items.

As a result, scanning devices—one of the key subprocesses of security access control—underwent significant development, advancing from what can be considered "Smart Airports level 1.0" to "Smart Airports level 2.0." In this context, it may be more accurate to refer to these advancements as part of "Smart Access level 1.0" and "Smart Access level 2.0." However, it is important to note that only two out of the eight security access control subprocesses mentioned in Table 1 remained unaffected by the introduction of X-ray technology.

Table 1. Access Control Technologies and Devices

Process of application	**Current technology / device**	**ML[1]**	**Future technology / device (Bridging the gap to Maturity Level 3.0 and 4.0 considering maturity areas)**
Validate Boarding card	• Digital handheld boarding card reader • Automated boarding card reader gate	2.0 2.0	• Sensors/camera's with biometric facial recognition Interconnection of systems will employ biometric recognition to ensure travelling passengers are granted access. Simultaneously registering passengers' presence into a database used by authorised stakeholders to enhance security and personalise passenger experience.
Pax enters Access Control queue	• Flexible queue management system • Passenger flow management system	2.0 2.0	• Advanced flexible queue & Advanced passenger flow management system Interconnection of systems allows guiding passengers from curb to gate based on their journey conditions. Encouraging just-in-time at various steps in the overall process and ensuring operational capacity is managed accordingly.
Information on Security process	• Displays with generic information	2.0	• Displays with personalized information based on enrolment info or mobile device token Utilizing passenger gained insights from i.e. biometric enrolment or token. Information can be optimised for understanding by passengers in managing the expectation of passengers at security screening. Decreasing the chance of delays and miscommunication by increasing exposure personalised instructions.
Divest	• Divest position allocation system (PAS) • Automatic tray return systems (ATRS)	2.0 2.0	• Personalized audio/video through facial recognition or mobile device language setting • Tray linked through biometrics Divest instructions is based on previously enrolled passport information to increase understanding of security process steps and reduce miscommunication. Biometric enrolled information is used to link passenger to belongings while being screened.

[1] Maturity Level

Passenger Screening	• Walk Through Metal Detector (WTMD) • Security Scanner / Body Scanner with Automated Threat Detection (ATD)	2.0 3.0	• State of art ATD algorithms & Attire recognition false alarm (FA) reduction algorithms • Biometrics data /screening result handling Advanced algorithms that analyse information gathered on the passenger background, biometric data, and attire. To perform risk assessment, threat detection, and aid security agents in targeted alarm resolution.
Belongings Screening	• X-ray machine with multi-view or Computed Tomography capability • Explosive detection system (EDS) algorithms • Central image processing (CIP) • Automatic Prohibited Item Detection System (APIDS)	2.0 / 3.0 3.0 3.0 3.0	• EDS, APIDS, CIP, CT • Screening result linked to pax with biometrics • No FA Advanced algorithms that analyse information gathered on the passenger background, biometric data, and attire. To perform risk assessment, threat detection, and aid security agents in targeted alarm resolution of passenger belongings. Simultaneously managing workload and capacity of screening agents deployed.
Re-check	• Explosive Trace Detection (ETD) • Liquids Explosive Detection System (LEDS)	2.0 3.0	• Verification through biometrics Enabling quick recognition for both passenger and security agents in the event of recheck baggage. Follow up actions for secondary screening indicated based on primary screening results whilst belongings are awaiting recheck. To allow quicker processing.
Re-claim	• Empty tray recognition systems (ETRS)	2.0	• Biometric link • Egress instructions Egress instruction utilising biometric recognition based on current progress within journey.

The terrorist attacks on September 11, 2001, were another key moment for airport security [11]. Airports worldwide implemented advanced screening technologies such as full-body scanners, capable of detecting non-metallic threats. These scanners use millimetre-wave or backscatter technology to create detailed images of passengers, revealing concealed objects that metal detectors might miss. This can be considered as another key indicator of the level of technological maturity in the security access control process. However, there is not yet an element to say that the Smart Access level 2.0 given by the full-body scanners is part of the Smart Access level 3.0., mainly because the sole change of the full-body scanner does not ensure a mature interconnection of the elements in the access control ecosystems allowing the use of digital data generated by the scanner and the sharing of information among the airport stakeholders and users for a more efficient management of the resources.

In the 2010s, biometric identification systems became increasingly prevalent across airports. Technologies such as fingerprint scanning, facial recognition, and iris scanning provide a higher level of security by accurately verifying the identity of passengers and staff [12]. These systems not only enhanced security but also streamlined processes, promoting the scanning devices to serve Smart Access Level 3.0. At this level, the capability to utilize data to automate operations and processes plays a pivotal role in increasing efficiency. For example, biometric verification automates and speeds up passenger boarding, reducing bottlenecks and human error.

Recently, the integration of automated security devices and the use of Artificial Intelligence (AI) has further revolutionized airport security, marking a transition toward Smart Access Level 4.0. Automated lanes equipped with advanced imaging technology and AI algorithms significantly accelerate the screening process while maintaining rigorous

security standards. These innovations are critical to upgrading access control systems to Level 4.0, where AI, data analytics, and automation work in unison to create seamless, self-sufficient airport operations.

4.1 The role of biometric technology in security access control

There are different technological solutions available to perform each of the activities in the access control process both, for the users, passengers and staff, and its belongings, and therefore, the importance of its proper identification and classification level. For this reason, the devices currently available and the trends of them being used in the emerging digital ecosystem should also be considered. One of the most prominent is biometric technology.

Currently, biometric technology is used for access control purposes in diverse airports, this could be in the form of iris, facial or fingerprint recognition, and the use of facial recognition in passenger security screening is being introduced by more and more airports. According to Kasim, Winter, Liu, Keebler, and Spence [13] using biometric-enabled devices provides seamless travel for passengers and data on passenger movements for airports. In addition, the United States Customs and Border Protection states that biometric technology has a positive effect on the passenger experience as well as time-saving advantages [14].

IATA Global Passenger Survey of 2022 captures the experiences and expectations of passengers. Indicating that 83% of passengers are willing to share data to expedite airport processes. Moreover, 93% of passengers are interested in a program to expedite security screening [15]. Looking at the findings of the IATA survey and other ones being executed by airports globally; it is inferred that the majority of passengers are ready for further steps to increase their travel experience. Dubai International Airport, Japanese airports, and Singapore Changi Airport are all paving the way for biometrics to become the standard in passenger travel [16, 17].

The implementation of biometric technology in airports aims to enhance both passenger convenience and security efficiency. It simplifies the passenger journey by providing necessary information and ensuring seamless processing at various checkpoints. Simultaneously, biometric systems support security agents in performing more effective control and screening of passengers by streamlining the verification process. Biometric identification offers a more secure method of verifying access credentials, eliminating the need for separate checks of boarding passes, passports, staff IDs, and service provider credentials. For instance, a staff member's facial biometric features can grant access to secure areas, such as airside operations or MRO (maintenance, repair, and overhaul) facilities, according to their level of authorization.

Abdulrahman & Alhayani [18] have summarized the key advantages and disadvantages of physiological and behavioral biometric technologies. One major advantage is the difficulty of imitation, making biometrics a secure authentication method. However, biometric systems face challenges due to the natural variability in human characteristics. Physiological or behavioural traits can change over time or due to temporary conditions such as injury, leading to potential recognition errors. The technology may struggle to authenticate individuals when such inconsistencies occur.

In the Smart Access level 3.0 and Smart Access level 4.0, security is approached with this integral vision based on real-time information sharing, and with the notion of self-service operating technology. This approach improves the scalability of the systems, providing capacity on demand, and triggering the handling of growing volumes of passengers while minimizing human involvement in the Access Control process. These solutions will produce more useful data which can be analysed to provide insights on operations, process management and optimization benefitting staff members and passenger experiences.

Biometric technology also facilitates risk-based screening, where passengers are screened according to the level of risk they pose. By capturing biometric data prior to screening, passengers can be verified against security databases containing pre-gathered, security-relevant information, helping security agents determine the appropriate level of screening needed [19]. Another recent study by Validivia, Serrajòrdia & Swianiewicz (2022) argues that biometrics are biased and will always be biased. Having looked into different studies published on understanding and mitigating bias in biometric systems focusing on demographic bias. This study highlights a concern that is also present in the technology used for aviation security purposes; where algorithms work on facial recognition, body shape, and other biometric physiological and behavioural characteristics.

Setting up such a system requires a large database, interconnected IT systems, data security, etc. The use of biometric technology poses diverse challenges and concerns for the privacy of passengers and the proper management of such sensitive data [20]. Special attention must be placed on Cyber Security due to the nature of the data and its amount, it becomes a target for cyber-attacks. Cyber-attacks may result from autonomous attacks and attacks based on solicited access, with the latter raising questions on authorized access levels and safeguards on data access and security. These emerging threats, next to the prevalent physical threat airports are constantly preparing against, require strategies and standards that guarantee the safeguarding of aviation [6, 21].

Future research could further examine what type of data is collected and how privacy and cyber security are impacted by the use of smart devices in Smart Access level 4.0. If, for instance, individual passengers can be identified based on data collected during security screening. There should be procedures in place to anonymize the data unless clear permission is given by the passenger. Such challenges could potentially hinder the quick formulation of regulation and policy for the development and implementation of e.g. biometric technologies, pre-screening, and artificial intelligence within Smart Access, even though the stakeholders are signalling what improvements are desired. Ultimately, the legislators on a global scale will need to define the rules.

Looking at an airport environment for the use of biometric technology means considering the design of the building and the location of processes and sub-processes where biometric technology can be implemented. The effects of the environment can be controlled to a certain extent. Another aspect to consider is the volume of passengers travelling through an airport. Swift processing of passengers is important from a safety and satisfaction perspective. However, the diversity of passengers creates a challenge for using biometrics. For example, do passengers have a travel/identification document containing their biometric characteristics which can be used during processing at the airport, or do passengers

enrol at the airport to prepare for processing. Ultimately, when used correctly biometric technology can enhance the passenger experience and the safety and security at an airport.

In addition, the technology used in aviation security is certified and meets global standards, different countries have different policies regarding the usage and application of these technologies [22]. The technologies implemented must meet specific legislative requirements and pass extensive testing for certification before being deployed. According to Sharma, Härtlein, and Marschner [23] the continuing development of digitalization is challenging existing business models as well as all business processes suggesting organisations such as airports assess their digital readiness through a Digital maturity model.

As previously mentioned, in the Smart Access level 3.0 and Smart Access level 4.0, security is approached with this integral or holistic vision, based on real-time information sharing among different stakeholders i.e. security providers, airports, airlines, or together agencies which in turn means having clear, transparent, up-to-date global security standards, and their proper adoption by the stakeholders.

The Airports Council International Europe (ACI Europe) with its working group known as the Security Technology Panel, has been looking into the requirements for the new digital ecosystem of technology used in the control access process (Airport Council International Europe). Whilst any innovation needs to meet the regulatory and legal requirements for Aviation Security, the document issued by ACI Europe expands the scope of the requirements to include the vision of the worldwide airport industry. Beyond this, it also describes the necessary properties of solutions to meet the future needs of various airports. These requirements allow manufacturers to gauge the level of readiness of innovations and to derive development roadmaps for current technologies.

Similarly, the Transportation Security Administration (TSA) has been working on its Biometrics strategy for Aviation Security & the Passenger Experience. Developing its strategy to facilitate technological development and the formulation of policies and standards [24]. In line with this strategy, TSA also created an Identity Management Roadmap for Transportation Security and the Credential Population and Passenger Experience. A roadmap with objectives that explore an identity management ecosystem to support the improvement of security effectiveness, passenger experience, and operational efficiency [25]. With ICAO as the leading aviation organization, on a global level steps are being taken in creating and adopting standards towards digital transformation in aviation security with the example of ACI and TSA mentioned above.

As presented in the previous section, it is proposed to address the level of technology adaptation by its maturity in different areas, and it should be important to incorporate these areas into the prerequisites mentioned above. In particular, the prerequisites of technology should include customer insight & experience-oriented to be acceptable to both airports and passengers while meeting the airports' needs. Therefore, the next subsection addresses the transition between Smart Access level 3.0. and Smart Access level 4.0.

5. The Transition between Smart Access Level 3.0 and Smart Access Level 4.0

One of the key advancements currently being developed is the use of data-driven automation, progressing towards Smart Access levels 3.0 and 4.0. The evolution and widespread adoption of sensing technologies, such as biometrics, combined with artificial intelligence, offer significant opportunities to enhance process efficiency and mitigate the impact of human error or inefficiencies [26-30].

However, a challenge remains in the biometric enrollment process. For algorithms to be precise and reliable, they must be trained on biometric data collected from a large, diverse population. Failure to account for demographic variability can introduce bias, making the system less accurate for certain groups. Additionally, challenges include the need for high-quality sensors to ensure accuracy and the substantial computational resources required to process biometric data effectively [31].

In the progression from Smart Access 3.0 to 4.0, one promising opportunity for increased efficiency lies in advanced data analytics, particularly through AI-enhanced detection systems. Currently, passenger screening is largely a rule-based, universal process [32]. However, AI's ability to detect non-obvious patterns and relationships in large datasets could significantly improve both the reliability and efficiency of passenger screening. By leveraging combined data and predictive analytics, AI can not only identify potential threats in unexpected ways but also streamline screening procedures, exemplifying the leap from Smart Access 3.0 to 4.0.

As previously mentioned, one of the trendiest technologies in the security access process is the use of biometric information for process automation of airport access [8]. At Smart Access level 4.0, the gathering of data on the passenger, within the boundaries of privacy regulation, creates opportunities to develop passengers' profiles based on specific characteristics. Often, biometric data is read from suitable passports in check-in or other access services; this data may include passport photographs, fingerprint information, but also other biometrics such as height [33]. Biometric data may also be gathered using sensors in a pre-screening step, provided that consent has been obtained from passengers. From a service aspect, it may be of interest to passengers to consider consent, if the process delivers improving the screening time and if it lessens the intrusiveness of the screening [34].

Figure 3 presents the pre-screening described above aiming to get passengers through security faster and more comfortably, by combining equipment from multiple stakeholders and the implementation of machine learning and/or deep learning algorithms, to enhance efficiency. After learning, the data gathered through pre-screening can be used to introduce personalized screening routes in a multi-vendor environment, which will improve the efficiency of the passage of the passenger. Since the sensors and currently available data sciences methods allow for the recording of many types of properties and/or biometric and attire information, upon which may be acted, there are unused opportunities for enhancing the efficiency of the security screening process. This exemplifies the pay-off for airports to adopt the Smart Access level 4.0: it provides an opportunity to improve efficiency, whilst it also improves passenger satisfaction.

Figure 2 outlines the key service concepts and systems that characterize Smart Airport 3.0 and 4.0 ecosystems. These systems are categorized into critical (white text) and non-critical (blue text) components. Critical systems are essential for achieving maturity at a given level, while non-critical systems may be incorporated to enhance functionality. As airports progress through higher maturity levels, the degree of system integration and interconnectedness increases.

Each technological advancement emphasizes the critical importance of accurate identification and classification within airport security systems. Effective access control relies on the ability to precisely distinguish between passengers, staff, and their belongings, ensuring that security measures are appropriately tailored to different levels of risk. Accurate identification enables early detection of potential threats, allowing airports to implement targeted security protocols that balance safety with operational efficiency. This section will delve into the role, key advantages, and challenges of biometric technology in security access control, highlighting how these innovations contribute to streamlined operations and enhanced security.

The service concepts, systems, and ecosystems of Smart Airport 3.0 and Smart Airport 4.0 vary in complexity and technological integration. These individual concepts can be categorized into "critical systems" (indicated by white text) and **non-critical systems** (indicated by blue text). Critical systems are essential for achieving the desired maturity level, while non-critical systems can be optionally incorporated to further enhance functionality. As airports progress to higher maturity levels, the degree of system integration and interconnectedness increases, resulting in more seamless, automated, and data-driven operations across the airport ecosystem.

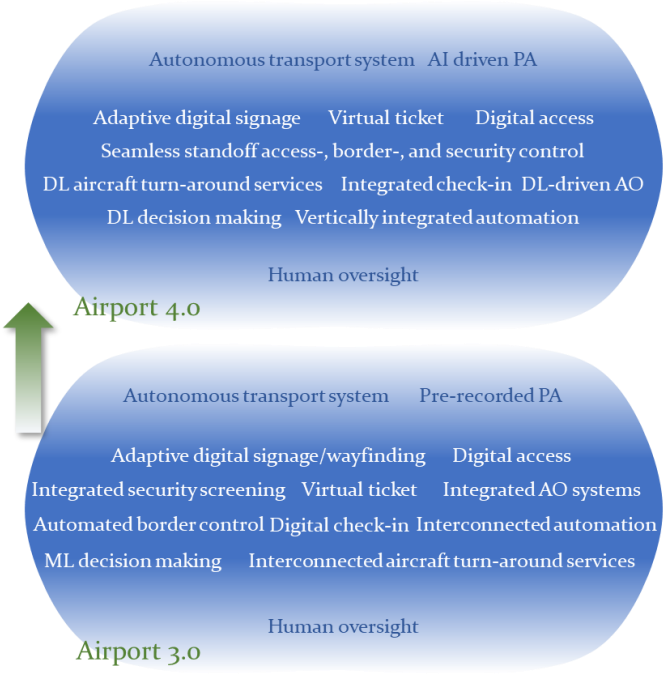

Figure 2. Service Concepts, Systems, and Ecosystem of Smart Airport 3.0 and 4.0

Level 3.0 Smart Airports demonstrate a shift towards more sophisticated technologies, incorporating early forms of automation, data analytics, and passenger self-service systems to improve operations. Airports such as Amsterdam Schiphol, Paris Charles de Gaulle (CDG), Dubai International, Munich, Zurich, and Istanbul fall into this category.

These hubs have adopted systems like self-service check-in, automated bag drop, and real-time flight information systems. Additionally, they use data-driven decision-making to enhance coordination among stakeholders, though the degree of interconnectivity and real-time automation is less comprehensive than in Level 4.0.

Level 4.0 Smart Airports, such as Doha Hamad, Singapore Changi, Seoul Incheon, and Tokyo Haneda, represent a fully mature digital ecosystem. These airports have seamlessly integrated cutting-edge technologies to optimize operations and improve passenger experiences. For instance, Doha Hamad International Airport (HIA) employs biometric verification, AI, and IoT to automate key processes. Its "Smart Security" initiative uses facial recognition and iris scanning to offer passengers a touchless experience. AI-driven systems manage real-time passenger flow and RFID technology combined with big data enhances baggage tracking.

Similarly, Singapore Changi Airport leverages AI, IoT, and robotics across multiple operational areas, including self-service check-in, baggage drop, security access, and energy management. Its digital ecosystem extends to a mobile app providing real-time updates and personalized services for passengers, optimizing both passenger convenience and resource management. Seoul Incheon International Airport leads in automation, deploying AI-powered "smart check-in" and "smart security" systems. Facial recognition technology and digital twins enable the airport to predict and mitigate operational disruptions. Incheon also employs AI chatbots and service robots to enhance customer service, while its digital twin technology aids in simulating and planning for potential operational bottlenecks. Tokyo Haneda Airport emphasizes cutting-edge automation with facial recognition enabling a touchless journey from check-in to boarding. The airport's real-time data-sharing infrastructure improves stakeholder coordination, and its AI decision-support tools optimize flight schedules and gate assignments. Like Incheon, Haneda also utilizes service robots and big data analytics to boost operational efficiency.

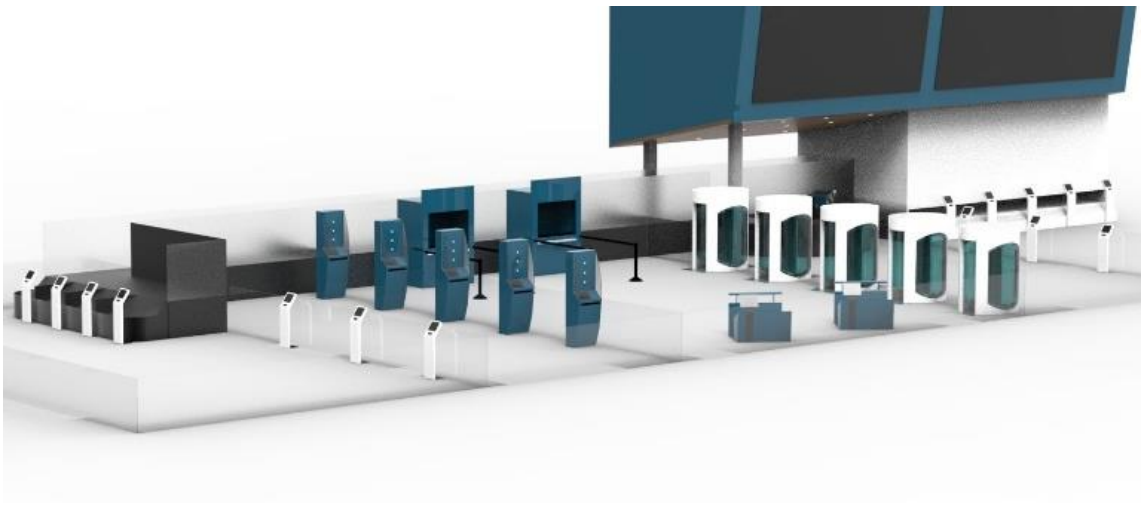

Figure 3. Pre-screening access control concept (SG11,2024)

A further enhancement of pre-screening may be tied to mobile devices which the passenger carries in the following way: Passengers could be invited to take e.g. a selfie in front of a suitable mirror, allowing them to prepare for screening as they are about to leave for travel, see Figure 3. By promising a more individualized and faster screening, their profiles could be pre-loaded and reconfirmed upon arrival at the airport by pre-screening sensors. By using phone location

information, after passenger consent, the airport would have detailed information of the passenger's travel progress to the airport and could both act towards the passenger and the airport operation with detailed actions. When passing through security, the phone could act as a token device, which allows the passenger to follow their screening path, to completion in a self-service manner. As such, this journey would conform to the Smart Airport 4.0 concept, and it will allow the airport and passengers to act at multiple levels of airport operation to enhance efficiency and passenger satisfaction.

The introduction of a personalized way of screening allows for categorization into predetermined passenger profiles if such simplification is necessary from a technological viewpoint. This categorization can for example be conducted based on the willingness of the passenger to provide certain personal information beforehand. The passenger would consent to share information that will accelerate access control and thus security screening.

Handling large amounts of personal data from passengers as well as operational data from airports and specifically airport security processes. Require a certain level of cyber security. Cyber threats and attacks are increasing in quantity, scope and complexity, where traditional detection and mitigation prove to be increasingly inadequate [35]. Higgins [36] reports on a recent cyberattack at Seattle-Tacoma International Airport that caused airport-wide outages and disruptions to operational critical systems. 64% of the 764 cyberattacks recorded in the aviation industry were aimed at airports to destabilize, reduce confidence, or exert geopolitical pressure [37].

To aid and reinforce in the detection of cyber threats and attacks, several Machine Learning and Deep Learning models are available and being developed to deal with current and future threats. Labu and Ahammed [38] categorized supervised and unsupervised Deep Learning frameworks and models that allow artificial intelligence to learn on command or based on a set of activities to constantly analyse datasets for emerging trends and fraudulent operations. Using frameworks as mentioned by Labu and Ahammed it becomes possible for airport to attain real-time and accurate detection of cyberattacks.

Future research could examine what type of data is collected and how privacy and cyber security are impacted through the use of smart devices. If, for instance, individual passengers can be identified based on data collected during security screening, the impact of that could infringe on passenger privacy. There should be procedures in place to anonymize the data unless clear permission is given by the passenger.

6. Conclusion

Digitalization and automation in airport processes, such as Access Control, are becoming increasingly prevalent, giving rise to the concepts of Smart Airports and Smart Access. This work aims to define and classify these concepts within a digital maturity taxonomy, which is structured around four key areas: Digital Vision, Digital Ecosystem, Digital Skills, and Customer Insight & Experience-driven services.

To demonstrate the value of this taxonomy, the Access Control process has been examined, with a focus on its associated digital ecosystems—i.e., the activities, devices, and technologies that enable a Smart Access process. Airport authorities can use this framework to assess their current level of digital maturity, while technology providers can use it to develop solutions tailored to specific maturity levels. Once the current status of digital maturity is established, airports can set clear objectives and take targeted actions in alignment with standards set by regulators and relevant authorities. Adhering to these standards fosters cooperation and compliance in an industry governed by stringent legislation and quality control measures.

For maximum effectiveness, close collaboration between airport authorities and technology providers is recommended to align strategic objectives with the limitations, capabilities, and development opportunities of the available technology. Several advanced technologies are already being used for security screening, including biometric systems, automated devices, and AI-powered decision-support tools that assist security personnel. AI algorithms, for instance, are employed to detect potential threat objects in passenger screening, and ongoing development aims to expand threat databases and improve object recognition capabilities. Integrated checkpoint management systems allow real-time monitoring of throughput performance, with AI providing data-driven decision-making support.

Lastly, challenges such as data security, privacy concerns, and the need for interconnected stakeholders underscore the complexity of digital transformation in airport environments, reinforcing the need for a thoughtful and collaborative approach to modernization.

Funding Details

This work was supported by BrightSky under Grant Rijksdienst voor Ondernemend Nederland (RVO) – R&D Mobiliteitssectoren (RDM). The authors would like to thank JetSupport B.V. for the opportunity to collaborate with industry partners on this study.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

1. Malik, H., et al., *A homomorphic approach for security and privacy preservation of Smart Airports.* Future Generation Computer Systems, 2023. **141**: p. 500-513.
2. Rubio-Andrada, L., et al., *Passengers satisfaction with the technologies used in smart airports: An empirical study from a gender perspective.* Journal of Air Transport Management, 2023. **107**: p. 102347.
3. Qi, Q. and Z. Pan. *Internet of things, internet, big data and airport services make smart airport based on o2o and humanism*. in *2018 International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2018)*. 2018. Atlantis Press.
4. Grodi, R., D.B. Rawat, and F. Rios-Gutierrez. *Smart parking: Parking occupancy monitoring and visualization system for smart cities*. in *SoutheastCon 2016*. 2016. IEEE.
5. Nau, J.B. and F. Benoit, *Smart airport how technology is shaping the future of airports.* Wavestone, Paris, 2017.
6. Jayasuriya, N. and A. Rajapaksha, *Smart Airport: A Review on Future of the Airport Operation.* 2020.
7. Teichert, R., *Digital transformation maturity: A systematic review of literature.* Acta universitatis agriculturae et silviculturae mendelianae brunensis, 2019.

8. ICAO, *Annex 17 - Security. Retrieved from icao.int: https://www.icao.int/casp-ap/Test%20Document/an17_cons.pdf#search=Search%2E%2E%2Eannex%2017*. 2017.
9. Commission, E., *Document 32010R0185. Retrieved from eur-lex.europe: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010R0185&qid=1686644738758*. 2010.
10. Panter, H.A., *Airport Security: Incidents That Changed Procedures*, in *Encyclopedia of Security and Emergency Management*. 2021, Springer. p. 1-9.
11. Klenka, M., *Major incidents that shaped aviation security.* Journal of transportation security, 2019. **12**(1): p. 39-56.
12. Panter, H.A., *Airport Security: Procedures in Secured Areas for TSA and Private Security*, in *Encyclopedia of Security and Emergency Management*. 2021, Springer. p. 9-17.
13. Kasim, K.O., et al., *Passengers' perceptions on the use of biometrics at airports: A statistical model of the extended theory of planned behavior.* Technology in Society, 2021. **67**: p. 101806.
14. Khan, N. and M. Efthymiou, *The use of biometric technology at airports: The case of customs and border protection (CBP).* International Journal of Information Management Data Insights, 2021. **1**(2): p. 100049.
15. IATA, *Global Passenger Survey 2022 media briefing. Retrieved from www.iata.org: https://www.iata.org/contentassets/baf7cb5eed64472aaac8906608085aff/global-passenger-survey-2022-media-briefing.pdf*. 2022.
16. Macalo, I.G., *How technology can cut airport queues. Retrieved from www.airport-technology.com: https://www.airport-technology.com/features/contactless-security-how-technology-cut-airport-queues/?cf-view*. 2021.
17. IDEMIA, *In Singapore's Changi Airport Terminal 4, IDEMIA fast and seamless travel. Retrieved from www.idemia.com: https://www.idemia.com/singapores-changi-airport-terminal-4-idemia-fast-and-seamless-travel?export=pdf&post_id=4430&force*. 2019.
18. Abdulrahman, S.A. and B. Alhayani, *A comprehensive survey on the biometric systems based on physiological and behavioural characteristics.* Materials Today: Proceedings, 2023. **80**: p. 2642-2646.
19. van Gaalen, P.e.a., *The future of passenger screening. Retrieved from www.pointfwd.nl: https://www.pointfwd.com/news/2021/3/8/the-future-of-passenger-screening*. 2021.
20. Zhang, Z. *Technologies raise the effectiveness of airport security control.* in *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*. 2019. IEEE.
21. Alabsi, M.I. and A.Q. Gill, *A review of passenger digital information privacy concerns in smart airports.* IEEE Access, 2021. **9**: p. 33769-33781.
22. ICAO, *Doc 10118 - Global Aviation Security Plan. Retrieved January 30, 2024, from www.icao.int: https://www.icao.int/Security/Documents/GLOBAL%20AVIATION%20SECURITY%20PLAN%20EN.pdf*. 2017.
23. Sharma, P., Härtlein, M., & Marschner, C, *Digital Readiness Assessment. Retrieved from assets.kpmg.com: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/ch-digital-readiness-assessment-en.pdf*. 2016.
24. TSA, *TSA Biometrics Strategy. Retrieved from tsa.gov: https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf*. 2018.
25. TSA, *TSA Identity Management Roadmap. Retrieved from tsa.gov: https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf*. 2022.
26. Fossum, E.R. and D.B. Hondongwa, *A review of the pinned photodiode for CCD and CMOS image sensors.* IEEE Journal of the electron devices society, 2014.
27. Lineback, R., *News & Bulletins. Retrieved January 30, 2024, from icinsights.com: https://www.icinsights.com/news/bulletins/cmos-image-sensor-sales-stay-on-recordbreaking-pace/*. 2018.
28. Miller, G., *The smartphone psychology manifesto.* Perspectives on psychological science, 2012. **7**(3): p. 221-237.
29. Russell, S., D. Dewey, and M. Tegmark, *Research priorities for robust and beneficial artificial intelligence.* AI magazine, 2015. **36**(4): p. 105-114.
30. Abadi, M., et al. {*TensorFlow*}*: a system for* {*Large-Scale*} *machine learning.* in *12th USENIX symposium on operating systems design and implementation (OSDI 16)*. 2016.
31. Lien, C.-W. and S. Vhaduri, *Challenges and opportunities of biometric user authentication in the age of iot: A survey.* ACM Computing Surveys, 2023. **56**(1): p. 1-37.
32. Parliament, E., *Regulation No 300/2008. Retrieved January 30, 2024, from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0300&qid=1677668181577&from=EN*. 2008.
33. *The Council of the European Union. (2004, December 13). Council Regulation No 2252/2204. Retrieved January 30, 2024, from eur-lex.europa.eu/: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:HTML#d1e39-1-1*.
34. ICAO, *Resolutions Adopted By The Assembly - 39th session- Provisional Edition. Retrieved January 30, 2024, from www.icao.int/: https://www.icao.int/meetings/a39/documents/resolutions/a39_res_prov_en.pdf*. 2016.
35. Vaiyapuri, T., et al., *Deep learning approaches for intrusion detection in IIoT networks–opportunities and future directions.* International Journal of Advanced Computer Science and Applications, 2021. **12**(4).

36. Higgins, G., *News. Retrieved from International Airport Review: https://www.internationalairportreview.com/news/226474/sea-airport-still-recovering-from-cyberattack/*. 2024.
37. Julien, D., *Blog. Retrieved from SysDream: https://sysdream.com/blog/dive-into-thre-cyber-threat-landscape-in-the-aviation-industry-2023/*. 2024.
38. Labu, M.R. and M.F. Ahammed, *Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning.* Journal of Computer Science and Technology Studies, 2024. **6**(1): p. 179-188.