International Journal of Social Science Research
ISSN 2327-5510
2025, Vol. 13, No. 3

# Impact of AI Security Technology on Performance Efficiency in ABU Dhabi Airport

Ahmed Salem Khalfan Mohammed Alnuaimi

Faculty of Technology Management and Business

Universiti Tun Hussein Onn Malaysia, Malaysia

Roshartini Omar (Corresponding author)

Faculty of Technology Management and Business

Universiti Tun Hussein Onn Malaysia, Malaysia

E-mail: shartini@uthm.edu.my

Received: August 23, 2025 Accepted: Nov. 2, 2025 Published: Nov. 11, 2025

doi:10.5296/ijssr.v13i3.23325 URL: https://doi.org/10.5296/ijssr.v13i3.23325

**Abstract**

In response to escalating global security demands and the rapid advancement of digital technologies, international airports are under increasing pressure to modernize their security infrastructure without compromising operational efficiency. Abu Dhabi International Airport, as a leading aviation hub in the Middle East, provides a strategic context for evaluating the transformative potential of Artificial Intelligence (AI) in enhancing security performance. This study examines the impact of AI-based security technologies on performance efficiency at Abu Dhabi International Airport, with a focus on the mediating role of technology adoption. Using Partial Least Squares Structural Equation Modelling (PLS-SEM), the research analyses data collected from airport security personnel to assess both the direct and indirect effects of AI implementation on operational performance. The findings reveal that AI-based security technologies significantly enhance both technology adoption and performance efficiency. Additionally, technology adoption is found to mediate the relationship between AI technologies and performance outcomes, suggesting that the success of AI implementation depends not only on the technology itself but also on user acceptance and integration. The model demonstrates strong reliability, validity, and moderate explanatory and predictive power. These results underscore the importance of aligning technological advancements with employee readiness and adoption strategies to achieve operational excellence in high-security environments like international airports.

**Keywords:** AI Security Technology, Performance Efficiency, Technology Adoption, Abu Dhabi Airport, PLS-SEM

## 1. Introduction

The aviation industry is experiencing a significant transformation through the integration of Artificial Intelligence (AI), particularly in the domains of security performance, operational efficiency, and service quality. At the forefront of this evolution is Abu Dhabi International Airport, a leading aviation hub in the Middle East. As security threats grow increasingly complex and passenger expectations continue to rise, the adoption of AI technologies has become essential for delivering a safe, seamless, and high-quality travel experience (Ahmed, 2025; Yiğitol, 2025).

Despite global advancements in AI deployment, Abu Dhabi International Airport continues to face critical challenges due to the limited and uneven integration of these technologies. The airport remains susceptible to issues such as security breaches, smuggling activities, and operational delays. Legacy systems and manual processes hinder the airport's capacity to respond to evolving threats in real time, thereby compromising both its security standards and operational efficiency (Chiang, 2025; Otieno, 2025).

AI technologies present advanced, data-driven solutions to these challenges. Tools such as intelligent surveillance systems, biometric verification, and anomaly detection enhance situational awareness and enable early identification of potential threats (Fan et al., 2025; Muhammad et al., 2025). For instance, facial recognition and fingerprint scanning streamline check-in and boarding processes, reduce human error, and accelerate passenger flow (Jain et al., 2025; Balasubramaniam et al., 2025). Machine learning algorithms embedded within anomaly detection systems identify suspicious behaviours, allowing security personnel to take proactive measures in real time (Khan & Khan, 2025).

Beyond security, AI significantly contributes to improving efficiency by automating screening processes, particularly in the analysis of X-ray images for luggage inspection. This reduces passenger wait times and alleviates congestion at checkpoints without compromising accuracy. Additionally, predictive analytics supports operational planning by forecasting potential disruptions and optimizing resource allocation based on real-time and historical data (Zong & Guan, 2025; Ahmed, 2025). These AI-driven capabilities generate cost savings while boosting overall performance outcomes (MoghadasNian & Mojavezi, 2025).

AI technologies also play an important role in enhancing service quality. AI-powered chatbots provide real-time assistance to passengers, reducing the dependency on human staff and improving customer satisfaction. The seamless integration of AI into security and service functions helps reduce the physical and psychological stress often associated with airport screening, thereby enriching the overall passenger experience (Ogunwobi, 2025).

However, the integration of AI is not without ethical and regulatory concerns. Since these systems process vast volumes of personal and behavioural data, issues related to privacy, data protection, and algorithmic fairness must be addressed. Abu Dhabi International Airport has acknowledged these challenges by aligning its AI deployment with international and national regulations, thereby reinforcing public trust in its systems (Önday, 2025).

Globally, airports and airlines have been rapidly adopting AI to improve operations. For

example, British Airways at Heathrow Airport uses AI for dynamic flight scheduling and resource optimization, while Harry Reid International Airport has implemented AI-powered screening systems that integrate with advanced CT scanners to detect prohibited items automatically, thereby improving both security and throughput (Yiğitol, 2025). Although the benefits of AI in aviation are widely recognized, there remains a lack of focused academic research exploring how AI specifically influences performance efficiency in airports such as Abu Dhabi International Airport. Existing literature has tended to address AI's role in aviation broadly, without examining its combined effect on security outcomes, operational processes, and passenger experiences within a cohesive framework (Kim & Kim, 2025).

This study addresses that research gap by investigating the impact of AI-based security technologies on performance efficiency at Abu Dhabi International Airport, with a particular focus on the mediating role of technology adoption. It evaluates how biometric security, predictive analytics, and intelligent surveillance technologies contribute to security enhancement, operational optimization, and improved passenger experiences. Furthermore, the study explores the ethical and regulatory implications of AI deployment in airport security, offering insights for both local stakeholders and international aviation authorities seeking to implement AI-based systems for sustainable security and operational excellence.

## 2. Literature Review

This literature review synthesizes scholarly and industry-based research to inform the development of a conceptual framework assessing the impact of AI-based security technologies on performance efficiency at Abu Dhabi International Airport. It critically explores the influence of three core AI-driven technologies: biometric security, predictive analytics, and intelligent surveillance, in reshaping airport security operations and driving enhanced performance outcomes (Ahmed, 2025; Fan et al., 2025; Önday, 2025).

These technologies have emerged as essential components in the modernization of airport security infrastructure. Biometric systems enhance identity verification accuracy and expedite passenger processing, leveraging AI tools such as facial recognition and fingerprint analysis to automate routine procedures (Jain et al., 2025; Balasubramaniam et al., 2025). Predictive analytics facilitates proactive threat detection and intelligent resource planning by processing vast amounts of historical and real-time data through machine learning and deep learning algorithms (Zong & Guan, 2025; Ahmed, 2025). At the same time, intelligent surveillance integrates computer vision and IoT technologies to enable real-time monitoring, behavioral analysis, and automated incident response (Fan et al., 2025; Muhammad et al., 2025).

Collectively, these technologies are designed to optimize airport operations by increasing detection accuracy, minimizing delays, and streamlining service delivery. These outcomes directly support performance efficiency, the dependent variable in this study, which encompasses operational speed, accuracy, and overall service quality (Kim & Kim, 2025; Otieno, 2025; MoghadasNian & Mojavezi, 2025).

Furthermore, the review highlights the mediating role of technology adoption, which significantly affects the extent to which AI technologies deliver measurable improvements.

As supported by prior research, the successful implementation of AI systems is influenced not only by technical performance but also by the level of organizational readiness and user acceptance (Yiğitol, 2025). Key factors such as system integration, staff training, acceptance, and usage rates determine whether AI solutions are effectively embedded into daily operations and achieve their intended outcomes. These core constructs, including AI-based security technologies, technology adoption, and performance efficiency, form the foundation of the proposed conceptual framework and are further examined in the following subsections.

### *2.1 Impact of AI-Based Security Technologies*

This study identifies three core AI-based security technologies that play a pivotal role in strengthening airport security and enhancing operational efficiency: biometric security, predictive analytics, and intelligent surveillance. These technologies represent the cutting edge of AI innovation in the aviation sector and are increasingly adopted for their ability to improve threat detection, streamline security procedures, and enable real-time, data-driven decision-making (Ahmed, 2025; Fan et al., 2025; Önday, 2025).

Each of these AI applications functions as an independent variable in this research, with a direct influence on airport performance efficiency. Their implementation contributes to faster processing times, heightened accuracy in risk identification, and more adaptive security responses (Chiang, 2025; Jain et al., 2025; Zong & Guan, 2025). The following subsections provide a comprehensive overview of each technology and its practical application within the airport security environment, forming the conceptual foundation for the study's analytical framework.

#### 2.1.1 Biometric Security AI-Technology

Biometric security plays a critical role in modern airport operations by enabling accurate, automated identification of passengers. Technologies such as facial recognition, fingerprint and iris scanning, and biometric-enabled boarding gates are increasingly adopted to streamline check-in, immigration, and boarding processes. These systems significantly improve both security precision and passenger flow efficiency (Önday, 2025; Jain et al., 2025).

The effectiveness of biometric applications is powered by advanced AI technologies, notably Machine Learning, Deep Learning, and Computer Vision. Machine learning algorithms analyse biometric patterns and continuously refine identity verification processes, while deep learning enhances the precision of facial recognition systems through high-dimensional data analysis (Khan & Khan, 2025; Balasubramaniam et al., 2025). Computer vision supports real-time image and video interpretation, enabling swift and accurate biometric matching across large volumes of passengers. In addition, AI-driven anomaly detection strengthens system integrity by identifying fraudulent identities or unusual behaviours that may pose security threats (Ogunwobi, 2025).

Together, these AI-driven innovations contribute to more reliable, efficient, and secure airport environments, reinforcing the integrity of passenger verification processes while promoting seamless travel experiences.

### 2.1.2 Predictive Analytics AI-Technology

Predictive analytics is a key component in enhancing airport security by enabling proactive risk management and data-driven operational decision-making. In airport environments, it is utilized to forecast security threats, analyse passenger behaviours, and optimize the allocation of personnel and technological resources. By anticipating potential disruptions before they occur, predictive analytics improves security responsiveness and supports uninterrupted airport operations (Ahmed, 2025; Yiğitol, 2025).

This capability is underpinned by several advanced AI technologies, including Machine Learning, Deep Learning, Reinforcement Learning, and the Internet of Things (IoT). Machine learning and deep learning algorithms process vast amounts of historical and real-time data to detect subtle patterns and generate accurate forecasts. Reinforcement learning contributes by enabling adaptive strategies based on trial-and-error learning from environmental interactions, especially in complex security scenarios (Zong & Guan, 2025). Meanwhile, IoT devices enhance situational awareness by continuously collecting and transmitting operational and environmental data across airport systems.

These AI-driven technologies elevate predictive analytics from a reactive tool to a strategic asset in airport security. Intelligent forecasting enables authorities to anticipate emerging threats and operational bottlenecks, while anomaly detection ensures rapid identification of irregular patterns in passenger behaviour or system performance (Ahmed, 2025; Zong & Guan, 2025). Behaviour modelling supports more nuanced risk assessments, and real-time data-driven decision-making allows for agile, context-aware responses to dynamic airport conditions (Yiğitol, 2025). As a result, predictive analytics plays an indispensable role in creating a more secure, efficient, and resilient airport ecosystem.

### 2.1.3 Intelligent Surveillance AI-Technology

Intelligent surveillance has become a cornerstone of next-generation airport security systems, offering real-time monitoring, automated threat detection, and enhanced perimeter control. These systems go beyond traditional CCTV by incorporating AI capabilities to detect suspicious behaviours, unauthorized access, and unattended objects, thereby enabling faster and more accurate security responses (Fan et al., 2025).

This advancement is made possible through the integration of Computer Vision, Machine Learning, Internet of Things (IoT), and Robotics. Computer vision enables video feeds to be analysed in real time, identifying objects, facial features, or unusual movements. Machine learning algorithms continuously improve detection accuracy by learning from surveillance data and adapting to new patterns. IoT devices, such as smart sensors and connected cameras, facilitate the seamless collection and transmission of surveillance data across various airport zones. Robotics contributes through the deployment of autonomous patrol systems, which can monitor restricted areas and respond to incidents with minimal human intervention (Muhammad et al., 2025). Leveraging these AI technologies, intelligent surveillance systems significantly enhance the airport's ability to maintain situational awareness, prevent intrusions, and ensure the safety of passengers, staff, and infrastructure.

### *2.2 Airport AI-Performance Efficiency*

Performance efficiency in the airport context refers to the speed, accuracy, and effectiveness with which airport operations and security procedures are conducted. It encompasses key outcomes such as reduced passenger processing times, enhanced accuracy in security screening, minimized operational delays, and overall improvement in service quality. These performance metrics are critical to maintaining high levels of passenger satisfaction, seamless airline coordination, and a strong reputation for safety and reliability (Kim & Kim, 2025; Otieno, 2025).

The integration of artificial intelligence technologies particularly in biometric identification, predictive analytics, and intelligent surveillance has emerged as a major driver of performance efficiency in modern airports. For instance, AI-powered identity verification systems streamline check-in and boarding processes by significantly reducing queuing times. Predictive analytics enable airport authorities to anticipate passenger flow patterns and operational disruptions, allowing for the timely deployment of resources (Chiang, 2025). Furthermore, intelligent surveillance systems powered by AI enhance situational awareness and enable rapid response to security threats, thereby minimizing operational standstills and improving overall safety (MoghadasNian & Mojavezi, 2025).

Collectively, these technological advancements optimize airport workflows, reduce reliance on manual interventions, and support the delivery of a seamless, secure, and customer-centric travel experience. Enhancing performance efficiency through AI not only reinforces the airport's competitive edge but also aligns with broader strategic objectives such as operational resilience, sustainability, and service excellence in the global aviation industry.

### *2.3 Mediating Role of AI-Technology Adoption*

Technology adoption serves as a crucial mediating variable in the relationship between AI-based security technologies and performance efficiency at Abu Dhabi International Airport. The effectiveness of AI solutions such as biometric security, predictive analytics, and intelligent surveillance depends not only on their technical sophistication but also on the degree to which these technologies are successfully adopted by airport personnel, systems, and processes (Ahmed & Sandhu, 2025; Jalil et al., 2025).

Key dimensions of technology adoption include system integration, staff acceptance, adequacy of training, and actual usage rates. High levels of adoption indicate a well-executed implementation strategy, where AI technologies are embedded into routine airport workflows and supported by personnel who are confident and capable of using them. Conversely, poor adoption often results in underutilized tools, process inefficiencies, and limited gains in performance (Liu, 2025).

In the specific context of Abu Dhabi International Airport, technology adoption plays a central role in bridging the gap between innovation and operational outcomes. It transforms AI from a theoretical solution into a practical tool for achieving measurable improvements in security, efficiency, and service delivery. When staff attitudes toward AI are positive and supported by training and readiness, the likelihood of effective usage increases significantly,

enhancing the overall impact of AI deployment (Emon & Khan, 2025; Liu, 2025).

Ultimately, the adoption of AI technologies serves as the mechanism through which digital transformation efforts are translated into sustainable improvements in airport performance. It ensures that AI investments lead not only to enhanced technological capacity but also to tangible value in daily operations, contributing to long-term organizational success (Ahmed & Sandhu, 2025; Jalil et al., 2025).

### *2.4 Formulation of the Conceptual Framework*

The conceptual framework presented in Figure 1 shows the conceptual framework illustrating the mediating role of technology adoption in the relationship between AI-based security technologies and performance efficiency at Abu Dhabi International Airport. This framework integrates perspectives from established organizational and technological theories to explain how the successful implementation and internalization of AI tools contribute to measurable improvements in airport operations (Xiong et al., 2025; Suradi, 2025).

At the core of the model are three AI-based security technologies: biometric security, predictive analytics, and intelligent surveillance, which serve as the independent variables. These technologies have been widely recognized for their potential to enhance security protocols, automate routine tasks, and support real-time decision-making in complex environments such as airports. However, consistent with the Technology-Organization-Environment (TOE) framework, the presence of these technologies alone is insufficient to ensure performance gains. Instead, organizational and environmental factors play a critical role in shaping the extent and effectiveness of AI adoption (Suradi, 2025).

To address this, the model introduces technology adoption as a mediating variable, capturing how AI tools are integrated into daily operations. This construct is grounded in the Technology Acceptance Model (TAM), which posits that user perceptions of usefulness and ease of use influence their willingness to engage with new technologies (Wang et al., 2025; Al-Momani & Ramayah, 2025). In this study, technology adoption is assessed through key indicators such as system integration, staff acceptance, training adequacy, and actual usage rates. These indicators reflect both the organizational readiness and the behavioral dimensions necessary to translate technological capacity into operational efficiency.

The dependent variable, performance efficiency, reflects the expected improvements in operational outcomes resulting from successful AI adoption. These include reduced passenger processing times, improved accuracy in threat detection, minimized delays, and enhanced overall service quality. Importantly, the model's focus on internal capability and strategic alignment resonates with the Resource-Based View (RBV) of the firm, which emphasizes that sustainable competitive advantage arises not merely from acquiring external resources, but from effectively integrating them with internal competencies and routines (Malhotra et al., 2025; Sandeep et al., 2025).

This conceptual model synthesizes insights from TAM, TOE, and RBV to provide a comprehensive, theory-driven explanation of how AI technologies can transform airport

operations. It suggests that while AI tools hold transformative potential, their full impact is realized only when mediated by effective organizational adoption and alignment practices. This integrated approach provides a practical framework for understanding the dynamics of digital transformation in airport security operations and offers strategic guidance for enhancing performance in similar aviation contexts (Xiong et al., 2025).

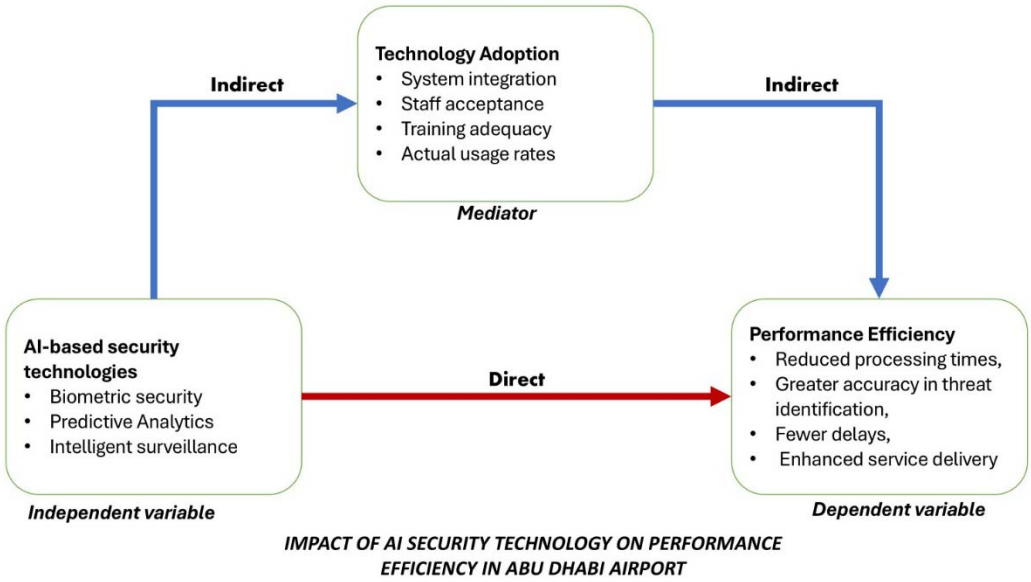


Figure 1. Established Conceptual Model

## 3. Methodology

This study employs a quantitative research design grounded in the established conceptual framework, which guided both the data collection and modelling procedures. A structured questionnaire survey was developed to measure the key constructs defined in the framework. The survey instrument was organized into sections corresponding to the independent variables (AI-based security technologies), the mediating variable (technology adoption), and the dependent variable (performance efficiency). Items were rated using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree), consistent with established norms in behavioural and social science research (Cohen, 1988).

The target population consisted of airport security professionals employed at Abu Dhabi International Airport. To ensure relevant expertise, the study targeted individuals with a minimum of two years of full-time experience in roles involving the implementation or use of AI-based security technologies. A simple random sampling method was adopted to ensure a representative and unbiased sample of the estimated population of 3,700 eligible professionals. Ultimately, 351 valid responses were collected and used for analysis.

The data were analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM) through SmartPLS software. PLS-SEM was chosen over covariance-based SEM (CB-SEM) due to several reasons. First, PLS-SEM is particularly suitable for exploratory

research and theory development, which aligns with the study's aim of proposing and empirically testing a new conceptual framework in the under-researched context of AI adoption in airport security (Hair et al., 2017; Sarstedt et al., 2020). Second, PLS-SEM is robust with smaller to medium sample sizes and is ideal for models involving multiple constructs and mediation effects, as in this study (Hair et al., 2019; Memon et al., 2021). Third, the approach is favoured when the primary objective is prediction and explanation of variance in key dependent variables, which fits the focus on performance efficiency (Zeng et al., 2021). Moreover, PLS-SEM accommodates non-normal data distributions and allows for formative and reflective constructs, offering modelling flexibility that is essential in real-world organizational research (Henseler, Ringle, & Sarstedt, 2015).

The analysis followed a two-stage approach. The first stage involved assessing the measurement model to establish the reliability and validity of each construct. Internal consistency was evaluated through Cronbach's alpha and composite reliability, while convergent validity was measured via average variance extracted (AVE). Discriminant validity was confirmed using the Heterotrait-Monotrait ratio (HTMT), which is recognized as a robust criterion in variance-based SEM (Henseler et al., 2015).

In the second stage, the structural model was assessed to determine the significance of hypothesized relationships, the magnitude of path coefficients, and the model's predictive relevance using $R^2$ and $Q^2$ statistics. The model was refined iteratively until acceptable levels of fit, reliability, and validity were achieved, ensuring a robust empirical representation of the conceptual framework (Aburumman et al., 2022; Hair et al., 2019).

Integrating PLS-SEM as the primary analytical technique, this study ensures methodological rigor and generates meaningful insights into the mediating role of technology adoption in the relationship between AI-based security innovations and airport performance outcomes.

## 4. Results of Analysis

The results of the PLS-SEM analysis are structured into two major stages: the outer model evaluation (measurement model) and the inner model evaluation (structural model). The outer model focuses on assessing the quality of the measurement instruments by examining the relationships between latent constructs and their associated observed indicators. This includes comprehensive testing of construct reliability using Cronbach's Alpha and Composite Reliability (CR) (Hair et al., 2019), evaluation of convergent validity through Average Variance Extracted (AVE) (Henseler, Ringle, & Sarstedt, 2015), and assessment of discriminant validity using both the Fornell-Larcker criterion and the Heterotrait-Monotrait (HTMT) ratio (Aburumman et al., 2022; Henseler et al., 2015).

Once the outer model satisfied the required validity and reliability standards, attention shifted to the inner model to test the hypothesized relationships between the constructs. This stage examined the path coefficients, t-values, and p-values to determine the significance and strength of each proposed relationship (Sarstedt et al., 2020). Additionally, the coefficient of determination ($R^2$) was evaluated to assess the model's explanatory power, while Stone-Geisser's $Q^2$ values were used to test predictive relevance (Hair et al., 2019; Zeng et al.,

2021). The model also examined mediation effects, particularly the role of technology adoption in the relationship between AI-based security technologies and performance efficiency (Sarstedt et al., 2020).

### *4.1 PLS Algorithm and Outer Model Evaluation*

The Partial Least Squares Structural Equation Modelling (PLS-SEM) algorithm was applied using SmartPLS software to estimate the path coefficients and assess the measurement (outer) model. This evaluation focused on examining the relationships between observed indicators and their corresponding latent constructs. PLS-SEM was selected for its robustness in modelling complex relationships involving latent variables and its suitability for exploratory research and predictive modelling (Hair et al., 2017; Hair et al., 2019). It is especially beneficial in contexts where the primary goal is theory development and where data distributions may not meet strict normality assumptions (Memon et al., 2021; Zeng et al., 2021).

The outer model assessment began with analysing indicator loadings, all of which exceeded the recommended threshold of 0.70. This indicates that each indicator strongly contributed to its respective construct (Hair et al., 2019). Construct reliability was then evaluated using both Cronbach's Alpha and Composite Reliability (CR), with all constructs demonstrating values above 0.70, confirming adequate internal consistency (Hair et al., 2017).

Convergent validity was assessed through Average Variance Extracted (AVE), with all constructs achieving AVE scores above 0.50, thereby indicating that a substantial proportion of indicator variance was captured by the underlying construct (Henseler, Ringle, & Sarstedt, 2015). To evaluate discriminant validity, both the Fornell-Larcker criterion and the Heterotrait-Monotrait (HTMT) ratio were employed. The Fornell-Larcker criterion confirmed that the square root of each construct's AVE was greater than its correlation with any other construct. Additionally, HTMT values for all construct pairs remained below the conservative threshold of 0.85, supporting strong discriminant validity (Henseler et al., 2015; Aburumman et al., 2022).

These assessments demonstrate that the measurement model meets the key criteria for reliability, convergent validity, and discriminant validity, thereby ensuring that the constructs used in the study are both statistically sound and conceptually distinct. Figure 2 shows the conceptual model after the PLS algorithm procedure was completed, depicting the standardized path coefficients and the structural relationships among the latent variables (Sarstedt et al., 2020).

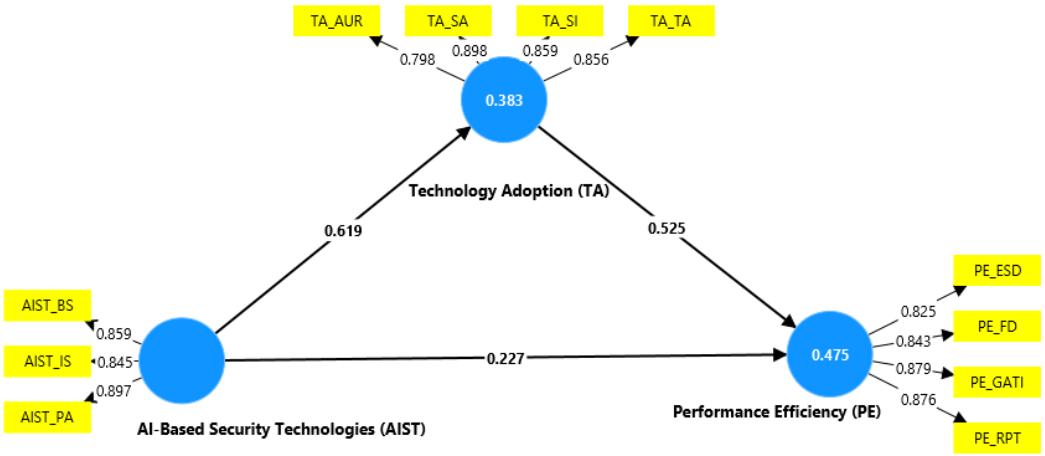


Figure 2. The model after PLS Algorithm procedure

Figure 2 illustrates the structural model output after applying the PLS algorithm. The model includes three latent constructs: AI-Based Security Technologies (AIST), Technology Adoption (TA), and Performance Efficiency (PE). The path coefficients indicate that AIST has a significant positive effect on both TA (0.619) and PE (0.227), while TA also positively influences PE (0.525), suggesting a mediating role. The $R^2$ values show that AIST explains 38.3% of the variance in TA and, together with TA, explains 47.5% of the variance in PE. Indicator loadings for all constructs exceed the recommended threshold of 0.70, supporting the reliability and validity of the measurement model.

Table 1. Construct reliability and convergent validity

| Constructs | Cronbach's alpha | Average variance extracted (AVE) |
|---|---|---|
| AI-Based Security Technologies (AIST) | 0.835 | 0.752 |
| Performance Efficiency (PE) | 0.878 | 0.733 |
| Technology Adoption (TA) | 0.875 | 0.728 |

Table 1 presents the results for construct reliability and convergent validity of the measurement model. The Cronbach's alpha values for all constructs, AI-Based Security Technologies (AIST) (0.835), Performance Efficiency (PE) (0.878), and Technology Adoption (TA) (0.875), exceed the recommended threshold of 0.70, indicating strong internal consistency reliability. Additionally, the Average Variance Extracted (AVE) values for all constructs are above the acceptable benchmark of 0.50, with AIST at 0.752, PE at 0.733, and TA at 0.728. These results confirm satisfactory convergent validity, showing that the indicators effectively represent their respective constructs.

Table 2. Heterotrait-Monotrait (HTMT) ratios

| | AI-Based Security Technologies (AIST) | Performance Efficiency (PE) | Technology Adoption (TA) |
|---|---|---|---|
| AI-Based Security Technologies (AIST) | | | |
| Performance Efficiency (PE) | 0.645 | | |
| Technology Adoption (TA) | 0.724 | 0.757 | |

Table 2 presents the Heterotrait-Monotrait (HTMT) ratios used to assess discriminant validity among the constructs in the model. All HTMT values fall below the recommended threshold of 0.85, indicating that the constructs are empirically distinct from one another. Specifically, the HTMT value between AI-Based Security Technologies (AIST) and Performance Efficiency (PE) is 0.645, between AIST and Technology Adoption (TA) is 0.724, and between PE and TA is 0.757. These results confirm that discriminant validity is established within the measurement model.

Table 3. Fornell-Larcker criterion

| | AI-Based Security Technologies (AIST) | Performance Efficiency (PE) | Technology Adoption (TA) |
|---|---|---|---|
| AI-Based Security Technologies (AIST) | 0.867 | | |
| Performance Efficiency (PE) | 0.552 | 0.856 | |
| Technology Adoption (TA) | 0.619 | 0.666 | 0.853 |

Table 3 presents the Fornell-Larcker criterion results, which are used to assess discriminant validity by comparing the square root of the Average Variance Extracted (AVE) for each construct with the correlations between constructs. For discriminant validity to be established, the square root of each construct's AVE (shown on the diagonal) should be greater than its correlations with other constructs (off-diagonal values). As shown, the square root of AVE for AI-Based Security Technologies (AIST) is 0.867, which is higher than its correlations with Performance Efficiency (0.552) and Technology Adoption (0.619). Similarly, Performance Efficiency (PE) has a square root AVE of 0.856, exceeding its correlations with AIST (0.552) and TA (0.666). Finally, Technology Adoption (TA) has a square root AVE of 0.853, which is greater than its correlations with AIST (0.619) and PE (0.666). These results confirm that all constructs exhibit satisfactory discriminant validity according to the Fornell-Larcker criterion.

### *4.2 PLS Algorithm and Model Fit*

The model fit was evaluated at the construct level using two key indicators: $R^2$ (coefficient of

determination) and $f^2$ (effect size). The $R^2$ value represents the proportion of variance in an endogenous construct that can be explained by its associated exogenous variables. It provides a measure of the model's explanatory power (Hair et al., 2019; Sarstedt et al., 2020). The $f^2$ value was used to assess the effect size of each exogenous construct by measuring its individual contribution to the $R^2$ value of the corresponding endogenous construct. According to Cohen (1988), $f^2$ values of 0.02, 0.15, and 0.35 represent small, medium, and large effects respectively.

Table 4. R-square values

| | R-square |
|---|---|
| Performance Efficiency (PE) | 0.475 |
| Technology Adoption (TA) | 0.383 |

Table 4 presents the $R^2$ (R-square) values, which indicate the proportion of variance in the endogenous constructs explained by their respective predictor variables. The $R^2$ value for Technology Adoption (TA) is 0.383, meaning that 38.3% of the variance in TA is explained by AI-Based Security Technologies (AIST). The $R^2$ value for Performance Efficiency (PE) is 0.475, indicating that 47.5% of the variance in PE is jointly explained by AIST and TA. According to commonly accepted thresholds, these values suggest a moderate level of explanatory power, confirming that the model has a reasonable ability to predict the endogenous constructs.

Table 5. f-square values

| | AI-Based Security Technologies (AIST) | Performance Efficiency (PE) | Technology Adoption (TA) |
|---|---|---|---|
| AI-Based Security Technologies (AIST) | | 0.061 | 0.622 |
| Performance Efficiency (PE) | | | |
| Technology Adoption (TA) | | 0.324 | |

Table 5 presents the $f^2$ effect size values, which indicate the magnitude of the impact that one latent construct has on another within the structural model. According to Cohen's (1988) guidelines, $f^2$ values of 0.02, 0.15, and 0.35 represent small, medium, and large effects, respectively. In this model, AI-Based Security Technologies (AIST) has a large effect on Technology Adoption (TA) with an $f^2$ value of 0.622, and a small effect on Performance Efficiency (PE) with a value of 0.061. Additionally, Technology Adoption (TA) shows a medium effect on Performance Efficiency (PE) with an $f^2$ value of 0.324. These results suggest that AIST strongly influences the adoption of technology, and both AIST and TA play meaningful roles in enhancing performance efficiency.

### *4.3 Bootstrapping and Hypothesis Testing*

Bootstrapping is a critical procedure in Partial Least Squares Structural Equation Modelling (PLS-SEM) that is used to assess the statistical significance of both direct and indirect relationships within the structural model. This non-parametric resampling method generates a large number of subsamples typically 5,000 or more, by randomly drawing observations from the original dataset with replacement (Hair et al., 2017; Sarstedt et al., 2020). Each subsample is used to re-estimate the model, allowing for the computation of standard errors, confidence intervals, and p-values for each path coefficient.

The technique is particularly useful in evaluating complex models with latent constructs, as it does not rely on the assumption of normal data distribution. In the present study, bootstrapping was employed to test the hypothesized relationships between AI-based security technologies, the mediating variable of technology adoption, and the outcome variable, performance efficiency. The statistical outputs from this process including t-statistics, p-values, and confidence intervals that indicate whether the hypothesized paths are statistically significant.

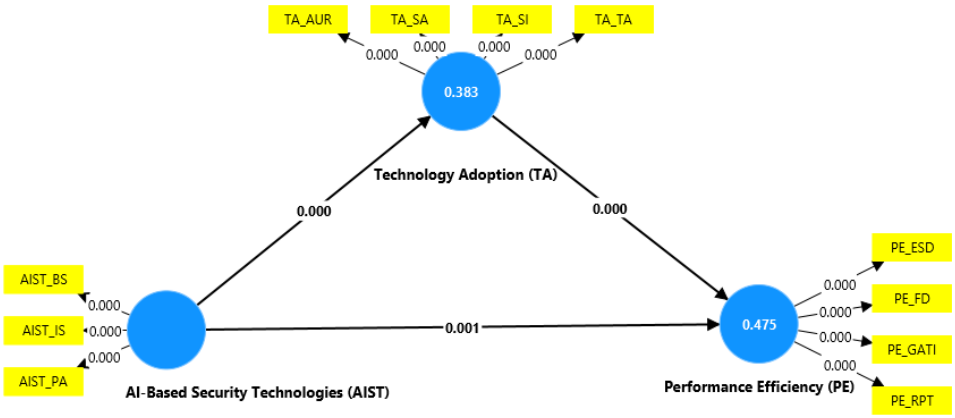


Figure 3. Graphical output of the bootstrapping procedure

Figure 3 illustrates that AI-based security technologies (AIST) have a significant direct effect on both technology adoption (TA) and performance efficiency (PE), with TA also showing a strong direct influence on PE. All path relationships and indicators are statistically significant ($p < 0.001$), confirming both direct and mediated effects within the model.

Table 6. Path strength and level of significance

| Direct relationship | Path strength | P values |
|---|---|---|
| AI-Based Security Technologies (AIST) -> Performance Efficiency (PE) | 0.227 | 0.001 |
| AI-Based Security Technologies (AIST) -> Technology Adoption (TA) | 0.619 | 0.000 |
| Technology Adoption (TA) -> Performance Efficiency (PE) | 0.525 | 0.000 |

Table 6 presents the results of the structural model analysis, highlighting the path strength and level of significance for the direct relationships between the key constructs. The findings indicate that AI-based security technologies (AIST) have a significant positive effect on both performance efficiency (PE) (path coefficient = 0.227, p = 0.001) and technology adoption (TA) (path coefficient = 0.619, p = 0.000). Additionally, technology adoption (TA) has a strong and significant positive effect on performance efficiency (PE) (path coefficient = 0.525, p = 0.000). All relationships are statistically significant at the 0.01 level, indicating strong support for the proposed model.

Table 7. Path strength and level of significance

| Indirect relationship | Path coefficient | P values |
|---|---|---|
| AI-Based Security Technologies (AIST) -> Technology Adoption (TA) -> Performance Efficiency (PE) | 0.325 | 0.000 |

Table 7 presents the result of the indirect relationship analysis, specifically examining the mediating effect of technology adoption (TA) on the relationship between AI-based security technologies (AIST) and performance efficiency (PE). The path coefficient for the indirect effect is 0.325, with a p-value of 0.000, indicating a statistically significant mediation. This suggests that technology adoption plays a crucial role in strengthening the influence of AI-based security technologies on performance efficiency, confirming its role as a significant mediating variable in the conceptual model.

### *4.4 Blindfolding and Predicative Relevance*

Predictive relevance evaluates a model's capacity to forecast the values of endogenous constructs accurately. In Partial Least Squares Structural Equation Modeling (PLS-SEM), this is assessed using the blindfolding procedure, which involves the systematic omission and prediction of data points to estimate how well the model performs on new or missing data (Hair et al., 2019; Memon et al., 2021).

Two main parameters are generated through this technique: Cross-Validated Communality (CCVC) and Cross-Validated Redundancy (CCVR). The CCVC focuses on the quality of the measurement model by assessing how well each construct's indicators can be reconstructed. The CCVR, in contrast, evaluates the predictive relevance of the structural model by incorporating both measurement and structural components (Sarstedt et al., 2020; Aburumman et al., 2022).

Table 8. CCVR values of the model

| | SSO | SSE | Q² (=1-SSE/SSO) |
|---|---|---|---|
| AI-Based Security Technologies (AIST) | 1194.000 | 1194.000 | 0.000 |
| Performance Efficiency (PE) | 1592.000 | 1051.239 | 0.340 |
| Technology Adoption (TA) | 1592.000 | 1155.117 | 0.274 |

Table 8 presents the Cross-Validated Redundancy ($Q^2$) values obtained through blindfolding to assess the model's predictive relevance. The $Q^2$ value for Performance Efficiency (PE) is 0.340, and for Technology Adoption (TA) is 0.274, both exceeding zero, indicating satisfactory predictive relevance for these constructs. In contrast, the $Q^2$ value for AI-Based Security Technologies (AIST) is 0.000, suggesting no predictive relevance for this exogenous construct, which is expected as predictive relevance primarily applies to endogenous constructs.

Table 9. CCVM values of the model

| | SSO | SSE | Q² (=1-SSE/SSO) |
|---|---|---|---|
| AI-Based Security Technologies (AIST) | 1194.000 | 617.014 | 0.483 |
| Performance Efficiency (PE) | 1592.000 | 731.536 | 0.540 |
| Technology Adoption (TA) | 1592.000 | 742.390 | 0.534 |

Table 9 displays the Cross-Validated Communality ($Q^2$) values, which measure the quality of the measurement model in predicting the indicators of each construct. The $Q^2$ values for Performance Efficiency (PE) (0.540), Technology Adoption (TA) (0.534), and AI-Based Security Technologies (AIST) (0.483) are all well above zero, indicating strong communality and confirming that the model has good predictive accuracy at the indicator level for all constructs.

Based on Table 8 and Table 9, it can be concluded that the model demonstrates satisfactory predictive relevance and communality for its key endogenous constructs. Specifically, the $Q^2$ values from Table 8 show that Performance Efficiency (0.340) and Technology Adoption (0.274) possess acceptable levels of predictive relevance, while AI-Based Security Technologies, being an exogenous construct, understandably shows no predictive relevance ($Q^2 = 0.000$).

Additionally, the high $Q^2$ values in Table 9 for AI-Based Security Technologies (0.483), Performance Efficiency (0.540), and Technology Adoption (0.534) indicate that the model also has strong predictive accuracy at the indicator level. Overall, the results support the model's robustness in predicting and explaining the variance in the observed data.

*4.5 Validated Framework and Discussion*

This section presents the validated framework developed from the modelling analysis of the conceptual framework, based on the empirical data processed using SmartPLS software, as illustrated in Figure 4.

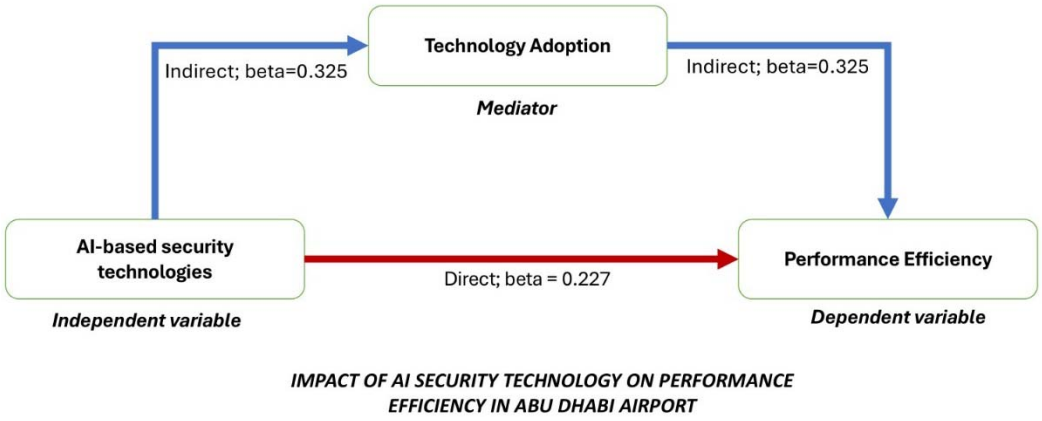


Figure 4. Validated framework

The validated conceptual framework illustrated in Figure 4 captures the structural relationship among AI-Based Security Technologies, Technology Adoption, and Performance Efficiency within the operational context of Abu Dhabi International Airport. This framework demonstrates both direct and indirect pathways, reinforcing the pivotal role of technology adoption in mediating the relationship between AI deployment and improved performance outcomes.

AI-Based Security Technologies, including biometric verification, intelligent surveillance, and predictive analytics, are shown to have a direct positive effect on Performance Efficiency, with a standardized path coefficient ($\beta = 0.227$). This finding is consistent with previous studies highlighting the ability of AI tools to streamline airport operations and improve threat detection and passenger flow (Jain et al., 2025; Ahmed, 2025; Yiğitol, 2025). These technologies independently contribute to faster screening, enhanced situational awareness, and optimized resource allocation, supporting findings from Otieno (2025) and Kim & Kim (2025), who emphasized AI's role in enhancing terminal efficiency and customer satisfaction.

Importantly, the model also confirms a significant indirect pathway from AI-Based Security Technologies to Performance Efficiency through the mediating role of Technology Adoption ($\beta = 0.325$). This aligns with earlier research by Emon and Khan (2025), Liu (2025), and Ahmed & Sandhu (2025), who demonstrated that user acceptance, readiness, and organizational integration significantly determine the extent to which AI technologies can deliver intended outcomes. The mediation effect underscores that technological innovation alone does not guarantee performance improvement; it must be supported by organizational

systems, adequate training, and a culture that promotes adoption.

Furthermore, the inclusion of Technology Adoption as a mediating construct is grounded in both the Technology Acceptance Model (TAM) and the Technology-Organization-Environment (TOE) framework. These theories posit that perceived usefulness, ease of use, and organizational readiness shape adoption behavior, which in turn influences performance (Wang et al., 2025; Al-Momani & Ramayah, 2025; Suradi, 2025). The Resource-Based View (RBV) also supports this conclusion by asserting that sustainable competitive advantages stem not merely from acquiring advanced technologies but from how well they are integrated with internal capabilities and human capital (Malhotra et al., 2025; Sandeep et al., 2025).

This validated framework provides empirical evidence that effective performance outcomes in AI-driven security environments are best achieved through a dual approach: deploying advanced AI technologies and cultivating strong adoption mechanisms. These results contribute to the growing literature on digital transformation in airport operations by integrating technology and human-centric implementation strategies into a unified explanatory model.

## 5. Conclusion and Implications

This study examined the impact of AI-Based Security Technologies (AIST) on employee-related performance outcomes, specifically Technology Adoption (TA) and Performance Efficiency (PE), at Abu Dhabi International Airport using Partial Least Squares Structural Equation Modelling (PLS-SEM). The empirical results confirm that AIST significantly and positively influences both TA and PE. Moreover, TA has a substantial direct effect on PE and also serves as a significant mediating variable, enhancing the impact of AIST on performance outcomes. These findings highlight the importance of promoting user readiness and effective integration when implementing AI-based solutions in operational settings.

The measurement model demonstrated strong psychometric properties, with all constructs exceeding the recommended thresholds for indicator reliability, internal consistency (Cronbach's alpha), convergent validity (AVE), and discriminant validity (Fornell-Larcker and HTMT criteria). The structural model exhibited moderate explanatory power, with $R^2$ values of 0.383 for TA and 0.475 for PE, and predictive relevance confirmed by $Q^2$ values above the 0.20 benchmark. Effect size analysis indicated that AIST had a large effect on TA, a small but meaningful effect on PE, and that TA exerted a medium effect on PE.

The practical implications of this study suggest that organizations, particularly those operating in high-security environments such as airports, should not only invest in advanced AI technologies but also focus on adoption strategies. These include providing targeted training, enhancing employee engagement, and ensuring organizational readiness to incorporate AI tools into core operational processes. Such measures are essential to convert technological investment into measurable performance outcomes.

From a theoretical perspective, the study contributes to the literature on AI implementation by

establishing Technology Adoption as a key mediating variable. It supports the integration of models such as the Technology Acceptance Model (TAM), the Technology-Organization-Environment (TOE) framework, and the Resource-Based View (RBV), offering a comprehensive understanding of how AI technologies influence organizational outcomes when combined with human and process factors.

Future research should explore additional mediating or moderating variables, such as organizational culture, digital literacy, or trust in AI systems, to expand the model's explanatory capacity. Validation across different sectors and geographical contexts would also enhance the generalizability and practical utility of the findings.

**References**

Aburumman, O. J., Omar, K., Al Shbail, M., & Aldoghan, M. (2022, March). How to deal with the results of PLS-SEM (pp. 1196–1206)? International conference on business and technology. Cham: Springer International Publishing.

Ahmed, A., & Sandhu, K. Y. (2025). Artificial Intelligence to Business Performance: A Mediation Model of Technology Adoption Readiness and Corporate Governance. *Journal of Asian Development Studies*, *14*(2), 1563–1577.

Ahmed, W. (2025). Artificial Intelligence in Aviation: A Review of Machine Learning and Deep Learning Applications for Enhanced Safety and Security. *Intelligence*, *3*, 100013.

Al-Momani, A. A. M., & Ramayah, T. (2025). Analysing EHR technology adoption: a comparative review of the technology acceptance model in different economic contexts. In *Intelligence-Driven Circular Economy: Regeneration Towards Sustainability and Social Responsibility* (Volume 1, pp. 327–344).

Balasubramaniam, S., Kadry, S., Prasanth, A., & Dhanaraj, R. K. (Eds.). (2025). *AI Based Advancements in Biometrics and Its Applications*. CRC Press/Taylor & Francis Group.

Chiang, C. H. (2025). AI in airport operations: Enhancing competitiveness and satisfaction. *Enterprise Information Systems*, *19*(3–4), 2454003.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioural Sciences* (2nd ed.). Lawrence Erlbaum Associates.

Emon, M. M. H., & Khan, T. (2025). The mediating role of attitude towards the technology in shaping artificial intelligence usage among professionals. *Telematics and Informatics Reports*, *17*, 100188.

Fan, W. Q., Ismail, A. S., Mohammed, F., & Mukred, M. (2025). AI-driven smart city security and surveillance system: A bibliometric analysis. In *Current and Future Trends on AI Applications* (Volume 1, pp. 305–328). Springer Nature Switzerland.

Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107–123.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modelling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135.

Jain, M. C., Bhawani, M. H., & Saxena, M. A. (2025). Enhancing biometric security with artificial intelligence: A cutting-edge approach. *IJSAT-International Journal on Science and Technology*, *16*(1).

Jalil, M. F., Lynch, P., Marikan, D. A. B. A., & Isa, A. H. B. M. (2025). The influential role of artificial intelligence (AI) adoption in digital value creation for small and medium enterprises (SMEs): does technological orientation mediate this relationship?. *AI & SOCIETY*, *40*(3), 1875–1896.

Khan, F. A., & Khan, M. K. (2025). Generative AI and Deepfake Detection in Biometric Systems. *Cognitive Computation*, *17*(3), 112.

Kim, Y., & Kim, C. (2025). A Study on the Efficiency of Airport Considering User Satisfaction. *Journal of Korean Society for Quality Management*, *53*(2), 221–236.

Liu, N. (2025). Exploring the factors influencing the adoption of artificial intelligence technology by university teachers: the mediating role of confidence and AI readiness. *BMC Psychology*, *13*(1), 311.

Malhotra, G., Dandotiya, G., Shaiwalini, S., Khan, A., & Homechaudhuri, S. (2025). Benchmarking for organisational competitiveness: a resource-based view perspective. *Benchmarking: An International Journal*, *32*(3), 943–964.

Memon, M. A., Ramayah, T., Cheah, J. H., Ting, H., Chuah, F., & Cham, T. H. (2021). PLS-SEM statistical programs: a review. *Journal of Applied Structural Equation Modelling*, *5*(1), 1–14.

MoghadasNian, S., & Mojavezi, S. (2025). *KPI-driven decision making in airport services: Enhancing operational efficiency, customer satisfaction, and sustainability*.

Muhammad, S. K., Ansari, T. A., Shabbir, B., Almagharbeh, W. T., Rehman, A., Arjmand, R., & Ghulam, A. (2025). The role of artificial intelligence in public health surveillance: A post-pandemic perspective. *Insights–Journal of Life and Social Sciences*, *3*(3), 74–80.

Ogunwobi, E. (2025). Advancing Financial Security Using Behavioural Biometrics and AI-Driven Authentication. *International Journal of Research Publication and Reviews*, *6*(3), 720–727.

Önday, Ö. (2025). AI-Driven Security System for Biometric Surveillance. In *Handbook of AI-Driven Threat Detection and Prevention* (pp. 290–307). CRC Press.

Otieno, S. (2025). Optimizing Airport Operations: A Study on Passenger Flow and Terminal Efficiency. *OTS Canadian Journal*, *4*(6), 86–96.

Sandeep, M. M., Lavanya, V., & Balakrishnan, J. (2025). Leveraging AI in recruitment: enhancing intellectual capital through resource-based view and dynamic capability framework. *Journal of Intellectual Capital*, *26*(2), 404–425.

Sarstedt, M., Hair Jr, J. F., Nitzl, C., Ringle, C. M., & Howard, M. C. (2020). Beyond a tandem analysis of SEM and PROCESS: Use of PLS-SEM for mediation analyses! *International Journal of Market Research*, *62*(3), 288–299.

Suradi, A. (2025). A Theoretical Extension of Technology Organization Environment (TOE) in E-Government: A Systematic Literature Review and Theory Evaluation. *Journal of Computer Science and Technology (JCS-TECH)*, *5*(1), 29–36.

Wang, Z., Wang, Y., Zeng, Y., Su, J., & Li, Z. (2025). An investigation into the acceptance of intelligent care systems: an extended technology acceptance model (TAM). *Scientific Reports*, *15*(1), 17912.

Xiong, S. H., Deng, Y. J., Zhang, H., & Chen, Z. S. (2025). Charting the path forward: a comprehensive barrier and solution analysis for digital transformation of small and medium-sized airports. *Enterprise Information Systems*, 2510347.

Yiğitol, B. (2025). AI, Robotics, and Autonomous Systems: Assessing AI Applications in Aviation Industry. In *Smart and Sustainable Operations Management in the Aviation Industry* (pp. 115–141). CRC Press.

Zeng, N., Liu, Y., Gong, P., Hertogh, M., & König, M. (2021). Do right PLS and do PLS right: A critical review of the application of PLS-SEM in construction management research. *Frontiers of Engineering Management*, *8*(3), 356–369.

Zong, Z., & Guan, Y. (2025). AI-driven intelligent data analytics and predictive analysis in Industry 4.0: Transforming knowledge, innovation, and efficiency. *Journal of the Knowledge Economy*, *16*(1), 864–903.

## Copyrights