



The Role of Smart Systems on Reducing the Recovery Time Objective “RTO” for Security Service Continuity in Airports: A Case Study of Dubai International Airport

Dr. Ahmed Mohamed Saleh Ahmed¹, Dr. Ibrahim Mohamed Alsaa'dy Elshreei²

¹Assistant Professor, Dubai Police Academy, United Arab Emirates, ²Associate Professor, Dubai Police Academy, United Arab Emirates

ARTICLE INFO

KEYWORDS

Smart Systems - Security Resilience - Crisis Management - Business Continuity - Recovery Time Objective “RTO” - Smart Airports - Dubai International Airport.

HOW TO CITE

Ahmed, D. A. M. S. (2026). The Role of Smart Systems on Reducing the Recovery Time Objective “RTO” for Security Service Continuity in Airports: A Case Study of Dubai International Airport. International Journal of Automation and Digital Transformation, 5(2), 112-128.
<https://doi.org/10.54878/24p21x40>

ABSTRACT

This research examines the role of smart systems in enhancing the continuity of security services and managing crises and operational disruptions in smart airports, with particular emphasis on their impact on reducing the Recovery Time Objective “RTO”. The research is grounded in the premise that the integration of smart systems extends beyond improving routine operational efficiency to becoming a critical enabler of dynamic security resilience during crisis situations. Using a descriptive-analytical approach, the study combines theoretical frameworks related to risk management and business continuity with an applied case study of Dubai International Airport as a high-density smart airport model. The findings demonstrate that the “security – operational” integration of automated screening systems, biometric identification technologies, self-service platforms, and command-and-control centers significantly contributes to reducing response time and RTO while maintaining decision accuracy and the continuity of critical security functions. The study concludes that smart systems represent a strategic pathway for strengthening security resilience in airports, supporting sovereignty requirements, crisis management capabilities, and the sustainability of security operations in highly sensitive environments.



Double-blind peer review by independent reviewers.

Received: 06 Jul 2026, Accepted: 17 Nov 2026, Published: 07 Dec 2026

*Corresponding author: dr.ahmed-mohammed@dubaipolice.ac.ae

Copyright: © 2026 by the author. Licensee Emirates Scholar Center for Research & Studies, UAE.

Open access under the Creative Commons Attribution (CC BY) license

<https://creativecommons.org/licenses/by/4.0>

Introduction:

Considering a changing world full of challenges and ambiguities, and the rapid and unpredictable development of smart technologies and artificial intelligence capabilities and applications, the risks facing security systems at airports have increased because of the widespread reliance on smart systems, including digital surveillance systems, and threat detection. and sudden interruptions, which can lead to the disruption of security services or a decline in their effectiveness at critical moments.

Based on the above, business continuity strategies in civil institutions of a security nature, especially airports and air ports, are no longer an option, but have become a matter of course that must be formulated accurately and competently so that they can prepare for all kinds of risks and crises and build scenarios and strategies in order to ensure the continuation of their business in the darkest conditions and the most accurate times.

The target recovery time has become a pivotal element in measuring the ability of airports to restore their security functions quickly and efficiently after a disruption or crisis, and this time has become a strategic indicator of the level of institutional readiness and resilience in the face of emergencies (Koryakina et al., 2021).

Since the UAE is the fastest growing Gulf country today, making it the most affected by international and regional external variables, these variables have a significant impact on the economic, social and security structure of the country. The UAE is also the barometer that measures the speed and pulse of these variables in the entire Gulf region. Therefore, the country must confront any challenge with strength and determination, because unless the country faces these challenges, it will affect the national security of the country (Elhegawy, 2021).

Security institutions have had to build sophisticated contemporary security strategies that are in line with the complex crisis environments and uncertainties that security decision-makers face when crises result in the interruption of security services.

As many global airports are moving towards adopting smart transformation strategies as an entry point to enhance their ability to withstand operational and security crises, by integrating artificial intelligence technologies and big data analysis within an integrated security system, we find that Dubai International Airport has surpassed many countries of the world in this regard, due to its widespread reliance on smart solutions in the fields of security inspection, crowd management, identity

verification, digital surveillance, and coordination between security authorities.

However, the question that came to the researcher's mind, based on his field experience in the field of airport security, is, "To what extent do these systems contribute to reducing the target recovery time in the event of breakdowns or crises?"

Based on the above, the researcher seeks to analyze the impact of smart systems on the target recovery time of the continuity of security services at airports - according to the available data and information - by applying to Dubai International Airport as a case study that represents an advanced operational environment in terms of technology and organization, and trying to find out the extent to which these technologies are able to reduce the target recovery time of security services at Dubai International Airport.

The Problem of the Study:

The main problem in this research appears in how to ensure the continuity of the effectiveness of security services at airports, in light of the growing nature of complex and overlapping risks to air ports, whether technical, operational or security risks, which may directly affect the ability of the security system at the airport to perform its vital functions without interruption, and this problem is becoming more complex in light of the increasing reliance on digital and smart systems in the management of security operations, which makes the "Recovery Time Objective" is critical in maintaining the continuity of the provision of security services efficiently and reliably.

There is an urgent need to adopt smart systems as essential support tools for managing security business continuity at airports, through their capabilities for early detection of failures, risk analysis and efficient management of security resources in times of crisis, in addition to their ability to build multiple operational scenarios to deal with partial or total failures of security systems, thus contributing to reducing the levels of uncertainty and uncertainty associated with the continuity of security services.

Accordingly, the problem of the study revolves around trying to analyze the impact of employing smart systems in enhancing the ability of the security system at airports to reduce the targeted recovery time for the continuity of security services, through an applied study on Dubai International Airport, as an advanced model in the use of smart technologies in the security field, where the study seeks to explore how security policies and procedures can be developed to ensure the continuity of the effectiveness

of security performance in the face of technical failures and emergency crises.

The problem of the study is crystallized in a major question: "What is the impact of smart systems on the targeted recovery time of the continuity of security services at Dubai International Airport?"

sub-questions emerge from this main question, the most prominent of which are:

- What are the smart systems used in managing security services at Dubai International Airport?
- What are the determinants of the target recovery time in the airport's security system?
- How do smart systems reduce recovery time when security services are disrupted?
- What are the main challenges facing the implementation of smart systems in achieving the continuity of security services?

The Importance of the Study:

The importance of this study stems from the novelty and vitality of its subject, due to its direct connection to the employment of smart systems in supporting the continuity of security services at airports, especially by focusing on the concept of targeted recovery time as a key indicator of the efficiency of the security system and its ability to recover quickly from malfunctions and crises. The study gains its objective importance from its attempt to contribute to the enrichment of the Arab scientific literature in the field of linking artificial intelligence and information technology on the one hand, and managing the continuity of security business in the airport environment from On the other hand, it enhances the theoretical understanding of the role of smart technologies in achieving security resilience and reducing the time effects of operational downtime.

The practical importance of the study is that it seeks to provide a theoretical framework that can be used by airport decision-makers when developing security policies and procedures related to recovery time and continuity of security services, through application to Dubai International Airport as an advanced model in the employment of smart systems in the field of security.

The results of the study may also help to highlight how smart technologies can be used to improve the speed of response to breakdowns and crises, and enhance coordination between security authorities within the airport, thus contributing to reducing the effects of disruption on air and passenger traffic, and enhancing

the ability of airports to maintain stable levels of security performance in various circumstances.

Objectives of the study:

The study aims to achieve a main goal of "clarifying the role of smart systems in reducing the target recovery time for the continuity of security services at airports", in a way that contributes to the development of security policies and procedures and enhances the flexibility of the operational security system.

To achieve this main goal, the study seeks to achieve a set of specific detailed objectives, the most prominent of which are:

- Define the conceptual framework for intelligent systems and security business continuity.
- Clarify the concept and importance of target recovery time.
- Clarify the role of smart systems in improving the speed of response to technical failures and emergency events within the airport environment.
- Studying the reality of employing smart systems in security services at Dubai International Airport and identifying their mechanisms of work and the extent to which they contribute to ensuring the continuity of security performance in emergency situations.
- Propose a set of future security policies and procedures that can support the optimal use of smart systems in reducing the target recovery time and enhancing the continuity of security services at airports.

Methodology:

The study relied on the descriptive-analytical method as the most appropriate scientific method for the nature of its subject and objectives, as this approach aims to describe the reality of employing smart systems in security services at airports - especially at Dubai International Airport - and to analyze the role of these systems in reducing the target recovery time for the continuity of security services in cases of operational failures or crises, in a way that allows the interpretation of the relationships between the study variables and the conclusion of scientific results within the limits of its objective framework and spatial.

Study Definitions:

Artificial Intelligence: It is the technology that enables computers to simulate human abilities such as

understanding, learning, and decision-making, making systems more capable of predicting and intelligently analyzing data (IBM, 2025).

- **Intelligent systems:** They can be defined as computer or electronics systems that possess sense, response, and control capabilities, enabling them to analyze situations and take adaptive actions based on available data (Worden et al., 2003).
- **Business Continuity:** It is defined as the situation in which an organization can continue critical operations during periods of interruption, breakdown, or disaster, and it requires initiative-taking planning and the implementation of flexible systems that ensure the availability of essential services (Speight, 2011).
- **Recovery Time Objective:** Recovery Time Objective is the maximum length of time a system or service can remain out of service before the impact of a downtime becomes unacceptable and is an important indicator in business continuity and disaster recovery plans (Almeida et al., 2021).

Limitations of the Study:

Objective Limitations: The study is limited to studying the impact of employing smart systems in reducing the target recovery time for the continuity of security services at airports, by addressing procedures related to the management of malfunctions and operational crises with a security dimension, without expanding the study of all types of risks or providing detailed solutions to all possible technical or security problems, as this falls within other research fields complementary to this topic.

Spatial Limitations: The study is based on Dubai International Airport as an applied field to analyze the impact of smart systems on the target recovery time of continuity of security services, as a model of an international airport that relies on smart technologies in managing its security and operational operations, with the possibility of benefiting from the results of the study in other airports of a similar operational and security nature.

Study Questions:

The study raises the following questions:

1. What are the smart security systems used at Dubai International Airport?

2. How is the target recovery time for security services calculated in cases of operational failures or crises in general, and at Dubai International Airport in particular?
3. To what extent do smart systems contribute to reducing the target recovery time for the continuity of security services at Dubai International Airport?
4. What are the most prominent technical and organizational challenges facing the use of smart systems to achieve continuity of security services at the airport?
5. How can security policies and procedures be developed at Dubai International Airport to maximize the use of smart systems in reducing the target recovery time?

Previous Studies:

A study titled "A passenger risk assessment method based on 5G-IoT" (Chen et al., 2021): The study aimed to develop a smart method for assessing passenger risk based on the integration of 5G and Internet of Things (IoT) technologies, with the aim of improving the efficiency of security systems in high-density environments such as airports. The study relied on collecting real-time data from sensors and cameras and analyzing it to classify passengers according to risk levels based on movement patterns and behavior. The results showed that the proposed model achieves a higher speed in detecting abnormal behaviors and better accuracy in assessing risks compared to traditional methods, thanks to the lower latency provided by 5G networks. The study concluded that the integration of 5G and IoT represents a promising entry point to enhance smart security, support the continuity of security services, and reduce delays in decision-making.

A study titled "How IGA Istanbul Airport leverages IoT and automation for improved efficiency, safety and passenger experience" (Yildiz et al., 2024): This study addressed how Istanbul International Airport (IGA) employs Internet of Things (IoT) architecture and automation systems to enhance operational efficiency, safety, and passenger experience within the airport. The airport relied on an integrated wireless network of smart sensors that are characterized by their speed, low cost, and long lifespan, and collect huge data from multiple points about operations. This data is used in big data analysis and predictive maintenance applications, enabling airport management to proactively improve performance rather than respond to after-events.

The results of the study showed that the use of smart IoT architecture contributed to improving customer satisfaction, enhancing predictive maintenance efficiency, reducing environmental impact, and increasing overall operational efficiency at the airport. These technologies have also helped to support operational decisions and improve the flow of operations in an integrated manner. The study discusses the benefits of IoT infrastructure and integration with other systems and highlights the role of automation in supporting the digital transformation of airport management.

A study titled "The Role and Applications of Airport Digital Twin in Cyberattack Protection during the Generative AI Era" (Weinberg, 2024): The study aimed to analyze the role of the Airport Digital Twin in protecting operational and security systems from cyberattacks in light of the escalation of generative AI capabilities that facilitate the design of more complex and adaptive attacks. The study started from the concept of the digital twin as a dynamic virtual model that simulates the real airport with its physical components, digital systems, and data flow in real time, allowing for an understanding of the complex relationships between operational and security systems.

The study explained that the employment of the digital twin provides a secure testing environment in which multiple scenarios of cyberattacks can be simulated, and their potential impact on critical systems such as surveillance systems, ground traffic management, telecommunications networks, and data platforms can be assessed. The digital twin also allows the effectiveness of response and recovery strategies to be assessed before they are implemented, reducing the reliance on direct experience in a sensitive operational environment such as an airport.

The results of the study concluded that the need to integrate the digital twin into the airport's cybersecurity system contributes to reducing the time to detect attacks and improve the speed of response, which reflects positively on protecting the continuity of vital services, especially security services. The study concluded that the digital twin is not just a technical tool, but an integrated platform that connects cybersecurity, crisis management, and strategic planning, enhancing the ability of airports to adapt to evolving digital threats and reduce their operational and temporal impacts.

Conceptual Framework for Smart Systems and Continuity of Security Services at Airports

Airports in the modern era have become complex operational systems in which the security and operational

dimensions overlap in a way that is difficult to separate from each other, which has made the process of managing security operations and illiterate decision-making a complex process that goes beyond the limits of traditional procedures based on the evaluation of the human element alone. Considering the escalating security threats and the increasing volumes of air travel, ensuring the continuity of security services has become one of the main pillars to maintain the safety of facilities and users, and to prevent the disruption of vital activities related to civil aviation.

Based on this, the researcher will try to build a conceptual framework that clarifies what smart systems are in the airport environment, while highlighting the nature of business continuity (security services) in that complex environment, as well as trying to define the concept of targeted recovery time as one of the most important indicators of continuity efficiency, through the following narrative..

What are smart systems in an airport environment?

Smart systems in the airport environment are one of the main pillars of the digital transformation system in the management of operations, whether operational or security, which means those systems that rely on artificial intelligence, the Internet of Things, and big data analysis to collect and process information and make decisions in near real-time (Chen et al., 2021).

The use of these technologies has contributed to the transition from traditional methods based on the human element alone to more accurate and flexible methods based on continuous monitoring and risk forecasting, as well as providing the opportunity to enhance security controls and improve the management of passenger and baggage flow.

Smart Systems in the Airport Environment:

The rapid growth in civil aviation traffic and the rise in air travel have helped to complicate the operational environment of airports in an unprecedented way, forcing airport security providers to look for new operational models capable of reconciling the requirements of security, operational efficiency, and the passenger experience, which has led to the emergence of a new security concept, namely "Smart Airport" "The process of relying on some advanced operational frameworks that generally rely on the integration of advanced digital technologies in the management of various operations (operational, organizational, security)" (Rajapaksha & Jayasuriya, 2020), and this transformation reflects the transition of airports from relying on traditional manual procedures to Intelligent systems are

based on data analysis and automation, allowing for more efficient resource management and rapid response to operational and security variables.

The researcher and the studies agree that this transformation was not just a technical development, but a radical change in the security philosophy of managing this vital facility, as its security and operational policy was no longer aimed at preventing the threat, but rather included a broader view, which is the ability to adapt to crises and ensure the continuity of business and vital services at all times (Mrňa, 2021).

Smart airports rely on an integrated digital infrastructure that employs IoT and automation to collect data from various operating points and then analyze it to support operational and security decisions, which has contributed significantly to improving passenger flow management in all conditions, as well as reducing waiting time and queues, and raising the efficiency of inspections and controls (Mrňa, 2021).

A recent study indicates that the latest development in the field of securing airports and ensuring the continuity of their business and security and operational functions is represented in the employment of a new concept called the "digital twin of the airport", which is based on a virtual model that simulates operational and security systems in real time, allowing to simulate malfunctions and cyberattacks and test response strategies in a secure environment before they are actually implemented. It shows that smart systems are no longer limited to temporary operation but have expanded into tools for strategic planning, risk management, and business continuity (Koroniotis et al., 2020).

Business Continuity "Security Services" in the Complex Airport Environment:

The continuity of security work at airports is one of the main pillars of the management of this facility, due to the sensitive nature of these facilities that cannot be interrupted or interrupted, and some went on to define it as "the ability of the security system to maintain an acceptable level of performance during crises, and the ability to quickly restore its basic functions after being exposed to a partial or total disruption (Bao et al., 2023).

This concept is closely related to risk and crisis management, which has become its most important basic principles after risk prevention operations, and has extended to reduce operational and temporal effects in the event of crises or risks, and various studies indicate that smart airports deal with the business continuity of their security services as part of national security and vital transportation, because of the consequences of any

disruption. The long-term economic, social and security impacts (Anagnostopoulou et al., 2024a), as well as studies based on cybersecurity crises at airports, indicated that the increasing reliance on digital systems has made the concept of business continuity a more complex system, as the interruption is no longer only caused by physical incidents or direct threats, but has also become linked to cyber breaches and sudden technical failures (Anagnostopoulou et al., 2024b).

How to Measure Target Recovery Time in Security Services in the Airport Environment:

The concept of Recovery Time Objective is a vital indicator used to measure business continuity efficiency, as it expresses "the maximum acceptable period of time during which a security service can be interrupted before the effects of a downtime become operationally and security unacceptable."

This indicator is particularly important in airports due to the close interdependence between security services and other operational processes such as aircraft movement and passenger flow, where the researcher agrees that the long recovery time reflects the weakness of the security, organizational and technical readiness of the organization, while its shortness reflects the high level of operational flexibility and the efficiency of crisis foresight in that organization. This shows that recovery time is not only a technical issue but is the product of an interaction between digital infrastructure, security policies, and the efficiency of human resources (Syahwami & Hamirul, 2024).

The Relationship between Smart Systems in the Airport Environment and the Target Recovery Time:

Some recent studies indicate that smart systems have a direct impact on reducing the target recovery time in different environments in general, and in the airport environment in particular, as they accelerate technical processes such as fault detection as well as significantly help them improve the quality of decision during a crisis, in addition to supporting operational reconfigurations after a downtime (Marshall et al., 2022), due to its superior capability in real-time data analysis, which allows locating the fault with greater accuracy and speed compared to traditional systems, and the studies explained that the combination of these systems with artificial intelligence has clearly contributed to building an early warning system for security failures, which reduces the scope of downtime and shortens the response time (Koroniotis et al., 2020). This confirms that the relationship between smart systems and recovery time is causal, as the high level of technical intelligence leads to

a decrease in the time needed to restore service, in addition to another study confirming that the digital twin allows to simulate recovery scenarios before the crisis occurs, reducing operational errors during the recovery phase and contributing to reducing the time needed to restart critical security systems (Rajapaksha & Jayasuriya, 2020).

The Role of Smart Systems in Reducing the Target Recovery Time of Security Services

Smart systems are gaining importance in supporting business continuity and security services at airports, due to their ability to reduce the targeted recovery time in cases of breakdowns or crises, as they rely on artificial intelligence and IoT technologies in the early detection of any malfunction or malfunction, through the use of real-time data analysis systems, which has helped security decision makers to Move from traditional response methods to simulation-based approaches and risk forecasting and containment before they worsen (Mustafa, 2023).

The researcher will try to highlight the role of these systems in reducing the target recovery time in security services, especially in times of downtime and crisis.

The Role of Smart Systems in the Early Detection of Failures and Security Threats:

The ability to detect malfunctions and security threats early is one of the most important factors affecting the reduction of the targeted recovery time of security services at airports, as the length of the recovery time is closely related to the speed of the detection of a defect or threat, and the researcher agrees with studies that confirm that smart systems based on artificial intelligence and the Internet of Things enable real-time monitoring of the operational environment, and analysis Data streams from cameras, sensors, and entry and exit systems, allowing anomalous patterns to be identified as they arise (Koroniotis et al., 2020).

One study indicates that networks of automated systems at airports, such as baggage handling networks or security screening systems, represent complex multi-component systems, and any partial malfunction in them leads to widespread disruption in security services, as it stressed the need to build models based on systems engineering and intelligent analysis of reliability, so that these models contribute to identifying vulnerabilities and weaknesses in the system to avoid them. before they turn into total failures, which allows for preventive intervention and reduced downtime (Anagnostopoulou et al., 2024b).

Another study also showed that the real-time simulation of queues at the airport "whether in the inspection areas and devices, in the waiting halls, or at the places where passengers deliver their baggage to the airlines" contributes significantly to the early detection of operational congestion zones, which would limit their transformation into a security or operational crisis, and prevent the accumulation of passengers at checkpoints, thus contributing to reducing the chances of security procedures disrupting in the event of any sudden malfunction (Marshall et al., 2022).

Early detection of problems or emergencies is no longer a technical function or security welfare but has become a strategic entry point to enhance security business continuity in these complex environments, as well as to help those in charge of these services reduce the target recovery time and return things to normal "resume at full strength".

The Importance of Smart Systems in Security Decision Support Operations During Crises:

Security decision-making during crises represents one of the most sensitive stages in the management of services at airports, due to what it encapsulates in a number of determinants such as "lack of time, multiplicity of alternatives, complexity or lack of available information", some studies have shown that traditional systems that rely on human experience alone suffer from a slowness in analyzing the situation. This will inevitably lead to a longer time required to choose the most suitable alternative, leading to a longer target recovery time (Mrña, 2021).

AI-based smart systems provide direct support to the decision-maker by analyzing operational and security data in real-time, simulating potential scenarios, and estimating the results of each alternative before it is actually implemented (Marshall et al., 2022; Rajapaksha & Jayasuriya, 2020).

Yildiz (Yildiz et al., 2024) point out that the use of the digital twin for airports enables security leaders to test response plans within a virtual environment that simulates operational reality, reducing the chances of error when implementing a decision in the actual environment, as well as reducing recovery time, as these decisions have been simulated and their results are known virtually before they are implemented, which enhances the effectiveness of the response and reduces organizational confusion during the crisis.

The researcher supports the trend that integration between actors in the smart environment is based on unifying efforts between operational and technical

entities and decision-makers through common digital platforms for real-time data exchange, which allows for improved coordination during crises and accelerating the process of responding to them (Hegawy, 2025).

The Importance of Smart Systems in Operational Reconfiguration Operations after Disruption:

Many studies confirm that the role of smart systems is not limited to the discovery and decision-making stages, but extends to the post-crisis stage, which is the stage in which operational configuration and the restoration of security services to their normal levels are carried out, and because this stage is the most influential in determining the target recovery time, due to the coordination between the different units, the redistribution of resources, and the restart of the damaged systems (Hegawy, 2025).

Studies that automation and IoT systems have contributed to accelerating predictive maintenance and restarting of malfunctioning equipment, by relying on sensor data and automated analysis of the status of systems, as well as their role in enhancing the transition from remedial maintenance to proactive maintenance, reducing downtime and shortening recovery time.

Cybersecurity studies at airports have also shown that the integration of artificial intelligence into digital incident response systems allows for the rapid isolation of infected systems, and the reconfiguration of affected networks without completely disrupting the rest of the security services (Anagnostopoulou et al., 2024b).

Challenges related to the employment of smart systems in the security field:

studies have indicated that the deployment of smart systems in airport environments – despite the multiple benefits in reducing the targeted recovery time – faces multiple challenges related to infrastructure, governance, and privacy as well as issues related to cybersecurity. Some researchers warn of the dangers of over-reliance on algorithms in environments that require highly sensitive human judgment such as airport security, as well as the emergence of a significant challenge related to the extent to which new intelligent systems can be integrated with legacy systems, which can sometimes lead to operational gaps that negatively impact the continuity of services if not systematically managed (Koroniotis et al., 2020).

The researcher agrees that the success of smart systems does not depend only on their technical efficiency, but also requires a legislative and regulatory framework that defines the controls of their use, protects the personal data of passengers, and ensures that automated decisions are subject to institutional accountability, as reducing the

target recovery time is not achieved by technology alone, but through the integration of technology with governance, training, and security policies (Kierzkowski et al., 2024).

The Proposed Conceptual Framework for the Relationship between Intelligent Systems and Target Recovery Time:

The researcher believes that the conceptual framework of this study assumes that there is a causal relationship between the level of employment of smart systems and the target recovery time of security services at airports, so that a higher level of technical intelligence leads to a decrease in the time required to restore service after a downtime. Some studies suggest that this relationship must be analyzed considering a set of intermediate variables, most notably the speed of fault detection, the quality of decision during the crisis, and the efficiency of operational reconfiguration after a failure (Dahake & Mirajkar, 2022).

In this context, smart systems are assumed to contribute to enhancing the continuity of security services through three main functions: the first is preventive which is represented in the prediction of risks before they occur, the second is operational which is represented in the support of the decision during the crisis, and the third is recovery which is represented in the acceleration of the restoration of service after a disruption, which results in the harmony and integration of functions to build a more resilient and resilient security system in the face of operational disruptions (Rauch & Hen, 2024).

The framework is an attempt to integrate the technical, administrative and security dimensions into a single analytical model, allowing the impact of AI and IoT to be understood not only as operational tools, but also as strategic elements in airport security management. The framework provides a theoretical basis for explaining how intelligent systems can reduce targeted recovery time and enhance business continuity and security services at major airports such as Dubai International Airport.

Analyzing the role of smart systems in reducing target recovery time at Dubai International Airport:

In recent years, Dubai International Airport has witnessed a significant expansion in the use of artificial intelligence technologies and digital command and control centers to support the continuity of critical services and reduce the effects of sudden failures. It has also helped to move from a traditional response to an initiative-taking one based on real-time analysis and risk forecasting (Al-Aklabi, 2017).

The researcher will try to analyze the role of smart systems at Dubai International Airport, by transferring their professional and practical experiences directly by following up on the security and operational mechanisms inside the airport, as follows...

Analyzing the role of smart systems in managing crises and security failures at Dubai Airport and its impact on reducing the target recovery time:

In order for the researcher to be able to analyze the role of smart systems in managing security malfunction crises at Dubai Airport, and measure the impact of this on reducing the target recovery time of security services, it was necessary to highlight some information related to the airport, so that the reader can know the size of the security operations that are carried out throughout the day, through the following...

About Dubai International Airport:

In 1960, Dubai International Airport was established as the city's first airport, with a single runway made of compacted sand and an area of 1,800 meters. The airfield served primarily as a station to refuel aircraft up to the size of the DC-3.

Since then, Dubai's leadership has promoted the growth of Dubai International Airport as both an airport and an aviation sector. Through a series of strategic expansion and development projects through DAEP, Dubai International Airport has grown and evolved in terms of passenger capacity, cargo capacity, aircraft movements, network of connected destinations, as well as operational efficiency. Two major projects were Terminal 2, which increased the number of passengers by two million, and Terminal 3, which increased the number to sixty million.

Dubai International Airport has retained the title of the world's busiest airport in terms of international passenger traffic since 2014 with a capacity of 115 million passengers per year. Dubai International Airport also ranks among the top ten international cargo hubs in terms of cargo volume with a capacity of 3.3 million tons per year.

In 2025, Dubai International Airport (DXB) recorded a new historic milestone in the global aviation sector, receiving 92.3 million passengers in 2024, the highest annual traffic rate in its history, surpassing the previous record of 89.1 million passengers achieved in 2018, cementing its position as the busiest international airport in the world (Dubai International Airport, 2026).

Smart Systems and their Role in Completing Security Operations at Dubai International Airport:

Dubai International Airport relies on an integrated system of smart systems that aim to speed up procedures,

enhance security, and achieve operational fluidity from the moment a passenger enters the airport until they board the plane.

The following are the most important smart systems used at Dubai International Airport:

Self-Registration Systems, Smart Gates & Security Checkpoints:

Self-registration systems at the smart gates at Dubai International Airport are one of the most important smart tools that are relied on in airport security operations, as their role is not only to facilitate travel checking, but also play a particularly important indirect security role.

Security-sensitive points, which would provide a greater opportunity to examine documents and documents, thus reducing the chances of tampering with documents or data, as well as the ability to create a unified digital record of passenger data that can later be linked to inspection and verification systems, these systems allow the integration of operational data with security analysis systems, which supports the early detection of unusual patterns, and contributes to the transition from interactive to proactive security (Alketbi, 2024).

In addition, smart gates equipped with Automated Tray Retrieval System represent a qualitative development in the philosophy of security inspection, as the inspection procedures have moved from a model based on human density to a model based on controlled automated flow, and its role is not limited to accelerating the process, but also performs a complex security function represented by:

- Reduce human friction processes and points.
- Prevent congestion – especially in checkpoints – that could turn into potential security risks.
- Standardize screening standards for all passengers and passengers, reducing disparities in security performance.
- Support real-time monitoring of pressure and flow levels within the checkpoints.

This system thus allows for the absorption of operational shocks caused by high passenger density or partial disruption of a route, without the collapse of the system.

Self-Baggage Drop Systems:

Baggage drop areas are always considered the most important and dangerous area in any airport, as they are the blind spot in all security control operations at airports, but the self-dropping systems at Dubai International Airport are one of the most important areas

in terms of security using the new artificial intelligence technologies, and the best of thermal and radiological inspection technology, and linking these technologies to smart applications capable of instantly analyzing the contents of those bags, and you find that these systems perform the following operations: (Automated Baggage Screening - Smart weighing and classification (instant linkage with baggage tracking systems) gives airport security officials full and secure control over a large number of passengers' luggage, and even the ability to link this baggage to passengers' personal devices, which would reduce direct contact with that baggage, as well as reduce human security errors, in addition to enhancing the safety of the baggage supply chain, and speeding up operations. Detect potential threats and ensure that unchecked baggage does not move into restricted areas (Al-Aklabi, 2017).

Biometric Recognition Systems (Facial & Iris Recognition Systems):

Biometric systems in passenger screening processes are the backbone of the smart security system at Dubai International Airport, as they allow the verification of the passenger's identity through multiple stages without the need to re-present documents, and their security importance lies in the following:

- Preventing plagiarism and forgery.
- Track the passenger's movement within the airport securely and without violating their privacy.
- Support immediate security decision when any unauthorized activities are suspected.
- Reduce action time while increasing accuracy.

From a crowd management perspective in high-sensitivity settings, these systems contribute significantly to controlling the human flow without creating tension or bottlenecks, which is a critical element of high-intensity events (Patel, 2018).

The role of smart systems and their role in managing crises and security failures and reducing the target recovery time at Dubai International Airport:

Based on the practical experience of the researcher at Dubai International Airport for a period of more than eight years, the experience of Dubai International Airport in the use of smart systems is evident during operational crises and security failures, where those in charge of Dubai International Airport – whether in charge of security operations, administrators or technical

technicians – were able to transform technical and operational integration from a tool to improve daily and operational performance, to an effective mechanism capable of restoring institutional control and reducing the target recovery time in the Crisis times whatever the crisis, situation, or event that the airport is facing.

In cases of labor disruption, technical failures, sudden increases in passenger densities, or limited security incidents, smart systems based on the integration of (automated inspection systems, biometric verification, baggage management) and command and control centers, work on real-time data exchange, which would enable the security decision-maker to quickly diagnose the source or sources of the malfunction and activate alternative routes without a complete disruption.

The smart system at the airport, which is based on the presence of more than one prevention point in the smart system, makes those in charge of following up the security operations able to prevent the crisis or problem from moving to the next stages (whether the problem is in the sorting points , inspection , follow-up and loading of bags, ...) by taking several measures, including:

- Automatically redirect human flows.
- Intensify smart monitoring of affected points.
- Real-time connectivity between systems and command centers supports risk-based decision-making.

This ensures business continuity at all points of the airport without disruption by seamlessly transitioning to emergency operating conditions while maintaining critical activities within shorter recovery times, in line with ISO 22301 requirements for continuity management and reducing the targeted recovery time for airport security services.

The researcher will explain some of the operational performance indicators that confirm that the return of smart systems in the context of crisis management is not limited to improving the speed of completion of transactions, but also extends to enhancing the ability to recover quickly, reduce response time, and increase the accuracy of security decisions, which consolidates the dynamic security resilience model that is able to absorb shock and restore readiness without losing institutional control in a highly sensitive sovereign environment.

Performance Indicators	Without smart systems	Using smart systems	Impact on target recovery time
Standby time at inspection during turbulence "Minute for passenger"	25 to 30 min	8 – 12	Reduce bottlenecks during emergencies
Processing time of the traveler in immigration during holidays in seconds	70 – 90 S	12 – 25 S	Accelerating transit despite operational constraints
Actual Capacity During the Crisis" Passengers per Hour"	100 – 130 passengers/hour	220 – 260 passengers/hour	Maintain flow and prevent partial downtime
Response time to a security incident is "in minutes"	15 – 20 min	4 -6 min	Real-time, data-driven decision
Target recovery time in minutes	90 – 90 min	25 - 35	Faster recovery and continuity for critical activities
Conversion rate for alternative routes	Limited	High	Fault isolation and prevention
Precision Verification While crowds	93 – 90%	97 – 99%	Reduce errors during peak
Command Center Readiness	Interactive	Initiative-taking	Risk-Based Crisis Management

The indicators confirm that the integration of smart systems at Dubai International Airport directly contributes to reducing the response time and target recovery time during crises and security failures, while maintaining operational efficiency and security accuracy.

This reflects the system's transition from reactive management to dynamic, flexible security management capable of absorbing shock and restoring readiness without losing institutional control.

Limitations associated with the use of smart systems in the security business continuity at Dubai International Airport:

The use of modern technology in the field of business continuity at Dubai International Airport – especially in crises – is not without technical, regulatory, legal and ethical challenges that may affect the effectiveness of these systems if they are not managed within clear governance frameworks, most notably over-reliance on technology, data protection and privacy issues, and ensuring the reliability of automated decisions in sensitive security contexts.

Institutional and operational controls that ensure the integration of smart systems with the requirements of business continuity and international standards for aviation security, as well as the use of this technology

within the framework of the legal and regulatory controls approved by the UAE and the corresponding human rights controls and guarantees to protect their personal life and freedom, in order to achieve a balance between operational efficiency and the requirements of legitimacy and justice.

The researcher has decided to summarize the presentation of these various challenges because they are not closely related to the research topic, and suffice to deal with only the most important ethical and technical constraints facing the process of using artificial intelligence through the following points:

Digital Privacy Violation:

Violation of digital privacy is one of the most prominent and serious ethical constraints associated with the use of artificial intelligence in airport security, as it has direct repercussions on societal trust and the moral legitimacy of those responsible for airport security and surveillance.

The main problem is that AI tools rely on the collection and processing of enormous amounts of personal data, whether explicit or implicit, often without the knowledge or explicit consent of the data owners (Syahwami & Hamirul, 2024).

Smart analytics tools rely on deep learning techniques, which store data in multiple layers that are difficult to track, making accounting or technical audits more complex, and increasing the likelihood of misuse or data leakage, whether intentionally or by cyber hacking.

Algorithmic bias:

Algorithmic bias is one of the most complex ethical and scientific challenges in the field of the use of artificial intelligence in security work in general and airport security in particular, as it has a direct impact on the integrity of the results and the credibility of the results drawn from them.

This bias refers to "those systematic deviations that appear in the results of algorithms because of the data on which they have been trained or because of the structuring of the models themselves" (Giordani, 2024).

This constraint is related to the effectiveness of crisis management and security decision-making in the UAE, as a breach of the principle of information fairness can lead to a misdiagnosis of the nature of the crisis or an inaccurate estimate of its magnitude.

In airport security, the competent authorities may rely on artificial intelligence systems to analyze the movements of individuals in the various halls, as well as to follow up on the movement of passengers, especially in the inspection and waiting areas, if the data contained in it has a certain bias against one of the groups, people or ethnicities, this may lead to unjustified alarm and may lead to unjustified crises, which would prolong the time allowed to practice security services, which entails exacerbating crises and mismanagement of the airport, which would fail all systems at the airport.

Systems Failures:

It can be defined as "the collapse of the components of the system, and its inability to fully perform the roles required of it (Shamsi, 2020)".

The failure of systems is different from partial inadequacy, which means "the inability of the system to perform one or more roles than its revolver", in partial inadequacy, a system is still able to perform some roles, whether primary or secondary, but when the system fails, the system is unable to perform anything and becomes both it and nothing.

Different causes of system failure: System failure occurs for one of three reasons(Shamsi, 2020):

- Application failure: This occurs either because the application "software" responsible for

running the system is corrupted or due to it being intentionally hacked or damaged.

- Failure of the communication network: As the entire system works as mentioned above using various communication systems "Wi-Fi - 5G - Bluetooth", and when that network fails to connect to the servers, in this case, the system will not be able to exercise the role required of it.
- Hardware failure: This type of failure is related to the entire infrastructure, and if one part of the infrastructure fails to function properly, it will consequently lead to the failure of the entire system, for example, a power outage from the main transformer or a failure of the main control panel.

Cyber Attacks:

It means "all unauthorized attempts to gain unauthorized access to systems, whether computers, operating systems or the like, either with the intention of altering their software in a way that serves the interests of the hacker, or to disrupt their work, or to steal certain data and information from them and exploit them for financial or personal benefits (Alibasic et al., 2017)".

The motive behind cyber-attacks varies according to the identities of the hacker, some of them are for political reasons with the aim of embarrassing the state and showing its inability to manage public utilities in it, and some of them are for personal reasons, as we have already mentioned, to obtain money through electronic extortion operations or to sell the information obtained from these attacks.

Different Images of Cyber Attacks:

There are many images taken by cyber attacks, which depend in their form and method on the type of target or weaknesses in the system, and in the following, the researcher will present the most important images of attacks that may be carried out on airport systems without addressing the forms of attacks that may occur on people.

- Distributed Denial Of Services DDoS attacks: These are "consecutive or simultaneous attacks carried out by an individual or some individuals by giving a large number of unimportant data or information to servers to the extent of so-called "information dumping" This will lead to slow services due to data congestion and the accountant's inability to process it fully, which

may sometimes lead to system failure and collapse." (Chahal et al., 2024).

- A Man-in-the-Middle (MITM) attack: This is one of the most popular types of hacks and attacks on systems, and this type of attack occurs when "a person, knowingly or unknowingly, places a computer or mobile application through an untrusted source, often loaded with Trojans or spyware. – Malware" and the user does not appear any problems during his use, but this software passes all the data and information through it, and thus the hacker has all the data that the user enters, such as "passwords, location, documents, confidential and non-confidential information, which later qualifies him to use them in a way that serves his personal interests." (Salem et al., 2022).
- Cyber Hijacking: In this type, the hacker accesses the computer or system in the same ways as he may use in the previous type, but in this case, he has full control over the system or electronic device, and the user cannot perform any operations on it.

This type of attack is often used to demand a ransom until the hacker regains control over the user of the device or service, and the value of the ransom is determined according to the amount of information and data obtained by the hijacker (the hacker) and its importance to its owner.

Exploiting Security Cameras Network: One of the most dangerous types of attacks that can occur on any airport is that a person or organization hacks into its surveillance camera system because in this case, he has a complete picture of the entire airport, and if he uses it to feed digital analysis systems linked to artificial intelligence technologies, he will be able to predict crises, disasters, and risks that these may face The airport or be aware of the movements of all persons in it, which would lead to the ability to plan for crises or disasters at the airport, and may increase their repercussions in a way that leads to the failure of the airport's systems entirely (Chen et al., 2020, 2021).

The inadequacy of the human element in performing its role:

Some may think that airport security is an existing system that works completely automated without the intervention of the human element, but this belief is wrong, because even if it relies on a smart system, it needs a qualified and trained human element to carry out the role assigned to it.

The more this component can deal with modern technologies and technologies, the better it will be for the airport security management process (Ramos et al., 2020) One of the most important forms of these problems or crises is the following:

The inability of the human element to deal with technology.

- Lack of training and qualification of the human element.
- The leak of the security and safety of the city and its proper management by the human element.
- Failure to oversee the data and information received from smart applications and technologies well.
- Intentional or unintentional human errors in the operation of the smart system.

Security Strategies for Dealing with These "Technical-Operational" Constraints at Dubai International Airport:

Since Dubai International Airport is one of the world's leading airports in this field of employing modern technologies in providing its services, it has not neglected how to deal with the "operational-technical" constraints that may occur in crisis situations, which would make the rebound time relatively longer than normal, and then we find that the airport's operational plan has adopted an advanced model in integrating smart systems within a highly efficient security system, and then the researcher will try to clarify the mechanisms Dubai International Airport avoids these restrictions in a way that enhances security continuity and reduces recovery time in emergencies.

Addressing Digital Privacy Violations:

Dubai International Airport (DXB) is tackling the issue of digital privacy by adopting an approach based on reconciling security requirements with the requirements for the protection of personal data, so that data collection is not seen as an end in itself, but rather as a functional means linked exclusively to the achievement of a legitimate security objective.

Accordingly, the design process of smart systems at the airport is based on the principle of "data minimization", so that the information necessary is used only to monitor risks or manage human flows without expanding the comprehensive tracking of individuals, as well as taking into account the process of separating operational data from metadata whenever possible, allowing behavioral and kinetic analyses to be carried out without direct

linking to personal identity except in cases of security necessity (Tahir, 2024).

This approach reinforces a strict system of control of powers, which prevents access to sensitive databases except by specific categories of operators, within the framework of regulatory policies that ensure compliance with national data protection and digital privacy legislation, and in a way that preserves the ethical legitimacy of the security system (Almeida et al., 2021).

Reducing the Effects of Intelligent Systems Failure:

Dubai International Airport addresses the risk of smart systems failure by adopting an operational policy based on technical resilience (more than one overlapping system) rather than relying on a single system, as the airport's digital infrastructure is designed on the basis of redundancy, ensuring that there is more than one operational path to perform the same security function, preventing a partial failure from turning into a full-blown collapse (Almarri, 2021).

Smart systems are also integrated into business continuity plans that include alternative operating procedures, whether manual or semi-automated, that are resorted to immediately after a digital system failure.

In addition, there are early warning systems to detect technical failures in their initial stages, which allow for rapid intervention before the malfunction worsens and turns into a large-scale operational crisis, which keeps recovery time within the acceptable operational and security limits.

Countering the Risks of Cyber Attacks

In dealing with cyber attacks, DXB starts from the perspective of it as an integral part of contemporary security risks, not just a separate technical threat, so smart systems are subject to multi-layered cyber protection measures that include data encryption, isolation of sensitive networks, continuous monitoring of information movement within the system, and strict policies are taken. It is about updating software and preventing the use of unsupported applications, to reduce the chances of penetrating systems via malware or "middleman" attacks.

In addition, there are also emergency cyber response plans that enable the rapid isolation of affected systems and prevent the attack from spreading to the rest of the airport's infrastructure, maintaining the continuity of security services even in the face of complex digital attacks (Florido-Benítez, 2024).

Addressing the inadequacy of the human element in the operation of the smart system

Dubai International Airport (DXB) understands that smart systems, no matter how advanced they may be, remain hostage to the efficiency of the human element that operates them and interprets their outputs, so those in charge of securing security services at the airport do not consider this smart transformation as a replacement for the element, but rather as a framework that supports its decisions and performance.

Therefore, the General Directorate of Airport Security relies on specialized training programs aimed at raising the efficiency of workers in dealing with digital technologies and analytical systems, thus reducing the chances of error resulting from misunderstanding or poor technical skill.

In addition to fostering an institutional culture based on responsibility and discipline through control systems that reduce the chances of leakage or misuse of security data, this integration between humans and technology leads to a reduction in operational errors, whether intentional or unintentional, and prevents human inadequacy from becoming a multiplier of crises at the airport.

Conclusion:

After the researcher completed the study of the research topic – through a combination of solid scientific references and the researcher's field experience within the environment of Dubai International Airport – she found that smart transformation is no longer a technological luxury, but rather a flexible structure whose value is measured by its ability to protect the continuity of security services in moments of turmoil. Analytical processing has shown that artificial intelligence, the Internet of Things, and command and control centers not only contribute to raising daily efficiency, but also reshape the concept of recovery in different crises and situations, transforming it from the concept of post-recovery to proactive recovery, and from delayed reaction to real-time data-driven decision.

However, this technological power carries within it ethical and operational limitations, and if these limitations are neglected, technology turns into a source of fragility instead of a source of protection, so the researcher emphasizes that the real value of the experience of Dubai International Airport lies in its ability to manage this delicate balance between speed and legitimacy, which is directly reflected in reducing the target recovery time and raising institutional readiness in the face of crises that may occur within it.

Results:

Reducing the target recovery time is not achieved through a single AI technology, but rather a series of

techniques and steps that contribute to the speed of discovery, the speed of diagnosis, the speed of decision, the speed of implementation, and then the verification of the safe return to service.

The study showed that the most dangerous aspect of bias is not the classification error itself, but the consequent sequential field decisions such as false alarms or unjustified referrals of passengers, as well as the drain of resources, which would prolong the recovery time even without an actual technical failure.

The study showed that the failure of smart systems becomes catastrophic when the leadership loses the ability to see accurately and in time, and thus the technical failure turns into a leadership failure in decision-making, which would expand the scope of the crisis and prolong the recovery.

The study confirmed that cyber threats are no longer separate conversations from smart environments – especially in airport security – but have become a threat affecting the operational determinants of the security services themselves, and may lead to the disruption of cameras, networks, or verification and identity systems, making continuity linked to the ability to quickly isolate and recover mechanisms and keep critical services running even during an attack.

The study concluded that the efficiency of training, operational discipline, and understanding of the outputs of intelligent systems determine whether the technology will reduce or increase the target recovery time, either due to mis operation, misinterpretation of early warning signs , or slow decision-making due to poor trust in the system, all of which are due to the efficiency of the human element in making the right decision at the right time.

Recommendations:

He believes that it is necessary to develop a detailed map of the target recovery time for each of the airport's critical security services, whether they are "passports and nationality, inspection, control, crowd management, communications", and define clear determinants to measure each of them, and link them directly to operational dashboards to ensure timely control of recovery.

It is recommended that the Human-in-the-Loop approach, which is intended for humans to actively participate in the operation or decision-making process of the intelligent system, to ensure that rights are not infringed or include restrictive measures, so that the algorithm remains an irreplaceable decision support tool,

with the aim of maintaining fairness and reducing the risk of bias that may create unjustified operational crises.

The study emphasizes that it is essential that there are daily operational procedures for cybersecurity related to continuity, including "rapid isolation - and partial recovery - operation of alternatives - with simulated drills for attacks on cameras, networks and identity systems" and measurement of recovery time for these actions and drills, because the recovery time in attacks is decided in the first minutes.

The study also emphasizes the need for the training programs to which airport workers are subjected to scenarios that represent the real pressures that may be faced during the performance of their tasks such as (camera failure, congestion, false alarm, penetration, system failure), with training the human element on decision-making mechanisms under time, as well as how to verify the outputs of artificial intelligence. So that it can make sure that its data is correct, and when it should switch to replacements in case of a breach or downtime.

It is recommended to adopt a fixed set of measurement indicators that can periodically measure detection time, response time, and false alarm rate, as well as calculate conversion time to alternatives, as well as safe return time, so that they can be linked to practical improvements.

References:

- Afroditi Anagnostopoulou et al. (2024). The Analysis and AI Simulation of Passenger Flows in an Airport Terminal, Sustainability, 2024, p. 1.
- Ali Bin Theeb Al-Aklabi, IoT Applications in Information Institutions. Alam, Arab Federation for Libraries and Information, 2017, Issue 19.
- Alibasic, A., Al Junaibi, R., Aung, Z., Woon, W. L., & Omar, M. A. (2017). Cybersecurity for smart cities: A brief review. In Data Analytics for Renewable Energy Integration: 4th ECML PKDD Workshop, DARE 2016... (pp. 22–30). Springer International Publishing.
- Almarri, G. A., Kamalrudin, M. A. S. S. I. L. A., Hakimi, H. A. L. I. M. A. T. O. N., & Sidek, S. A. F. I. A. H. (2021). Factors influencing human centric model for better passenger experiences using smart security system in Dubai airport. Journal of Theoretical and Applied Information Technology, 99(4), 976–986.
- Almeida, D, Shmarko K, Lomas E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a

- comparative analysis of US, EU, and UK regulatory frameworks. *AI Ethics*, 2(3), 377–387. doi: 10.1007/s43681-021-00077-w. Epub 2021 Jul 29. PMID: 34790955; PMCID: PMC8320316.
- Anagnostopoulou, A., Tolikas, D., Spyrou, E., Akac, A., & Kappatos, V. (2024). The analysis and AI simulation of passenger flows in an airport terminal: A decision-making tool. *Sustainability*, 16(3), 1346. <https://doi.org/10.3390/su16031346>
- Aruna Rajapaksha & Nisha Jayasuriya (2020). Smart Airport: A Review on Future of the Airport Operation, *Global Journal of Management and Business Research*, 2020, p2.
- Chahal, J. K., Bhandari, A., & Behal, S. (2024). DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review, and research challenges. *Computer Science Review*, 53, 100644.
- Chen, C., Surette, R., & Shah, M. (2021). Automated monitoring for security camera networks promises from computer vision labs. *Security Journal*, 34(3), 389–409.
- Chen, W., Huang, Y., Yang, H., Li, J., & Xianfeng, L. (2021). A passenger risk assessment method based on 5G-IoT. *Eurasip Journal on Wireless Communications and Networking*, 2021(1), 1–20. <https://doi.org/10.1186/S13638-020-01886-Z>
- Dahake, R., & Mirajkar, P. Integration Tool using Internet of Things in Smart Architecture of Passenger Processing at Airport Terminal.
- Digital transformation and resilience in airport operations: A systematic literature review. *Journal of Air Transport Management*, 109, 102379. <https://doi.org/10.1016/j.jairtraman.2023.102379>
- Dominik Mrňa & Benedikt Badánik (2021). Internet of Things as an Optimization Tool for Smart Airport Concept, *European Transport*, Issue 82, p.1.
- Dunka, V., Yerneni, R. P., Punukollu, M., Burugu, S., Punukollu, P., & Kodali, S. (2023). AI-Driven Disaster Recovery Optimization in Distributed Cloud Systems: Leveraging Predictive Analytics for Faster Recovery Time Objectives. *American Journal of Data Science and Artificial Intelligence Innovations*, 3, 68–73.
- El Hegawy, Ehab. Foreseeing the Security Policies of the United Arab Emirates to Face Future Regional Challenges, *Scientific Journal, Faculty of Commerce, Assiut University*, Issue Seventy-Two, 2021.
- El Hegawy, Ehab. Organizational Resilience in Smart Cities: A Comparative Analysis of Dubai's Experience and Several Global Centers, *Journal of International Crisis & Risk Communication Research*, 2025.
- Florida-Benítez, L. (2024). Identifying and classifying cyberattacks on airports. *Cyber Security: A Peer-Reviewed Journal*, 8(1), 63–79.
- Giordani, J. (2024). Mitigating chatbots AI data privacy violations in the banking sector: A qualitative grounded theory study. *European Journal of Applied Science, Engineering and Technology*, 2(4), 14–65.
- Kierzkowski, A., Kisiel, T., Mardeusz, E., & Ryczyński, J. (2024, December). Analysis of the Possibility of Using Eye-tracking in Evaluating the Work of an Airport Security Control Operator. In *2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 237–241). IEEE.
- Koroniotis, Nickolaos et al. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports, *IEEE Access*, Vol. 8, p. 209803.
- Koryakina, A. S., Gryzunov, V. V., & Burlov, V. G. (2021). Ways to Reduce the Time of Response to Threats to an Airport. *IFAC-PapersOnLine*, 54(13), 97–102.
- Marshall, Z. A., Mott, J. H., Gottwald, A. J., Patrick, C. A., & Dy, L. R. I. (2022). Expediting airport security queues through advanced lane assignment. *Journal of Transportation Security*, 15, 245–262. <https://doi.org/10.1007/s12198-022-00247-9>
- Mustafa Sabah Mustafa, The Process of Tracking the Movement of an Object in the Field of Computer Vision, Ph.D. Thesis, Faculty of Information Technology, University of Babylon, 2023.
- Ramos, A., Adrielly, N., Soler, A., Francisca, I., Idalia, F. M., & Jéssica, L. M. (2020). Designing human mistake-free machine: A Mexico City public transport commuters' approach. *Procedia Manufacturing*, 42, 399–405.
- Rauch, R., & Hen, C. (2024). From bricks to bytes: AI-based airport digital transformation in practice. *Journal of Airport Management*, 19(1), 83–95.
- Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., & Boutaba, R. (2021). Man-in-the-middle attack mitigation in internet of medical things. *IEEE Transactions on Industrial Informatics*, 18(3), 2053–2062.
- Shamsi, J. A. (2020). Resilience in smart city applications: faults, failures, and solutions. *IT Professional*, 22(6), 74–81.
- Speight, P. (2011). Business continuity. *Journal of applied security research*, 6(4), 529–554.

Syahwami, S., & Hamirul, H. (2024). The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia. *Enigma in Law*, 2(2), 75–84.

Tahir, G. A. (2024). Ethical Challenges in Computer Vision: Ensuring Privacy and Mitigating Bias in Publicly Available Datasets. *arXiv preprint arXiv:2409.10533*.

Weinberg, A. I. (2024). The Role and Applications of Airport Digital Twin in Cyberattack Protection during the Generative AI Era. <https://doi.org/10.48550/arxiv.2408.05248>

Worden, K., Bullough, W. A., & Haywood, J. (2003). *Smart technologies*. World Scientific.

Yildiz, B., Aydemir, M., Hisarkaya Kurnaz, C., Arslan, H., & Öz, K. (2024). How IGA Istanbul Airport leverages IoT and automation for improved efficiency, safety, and passenger experience. *Journal of Airport Management*. <https://doi.org/10.69554/pqif1520>

Zachary A. Marshall et al. (2022). Expediting Airport Security Queues through Advanced Lane Assignment, *Journal of Transportation Security*, 2022, p. 247.