Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i04.047

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Artificial Intelligence-Enabled Airport Security Systems in Saudi Arabia: Supporting Safe and Smart Aviation under Vision 2030

Taimoor Shahid Malik[1*]
[1]Consultant, Airport Special Systems, Jeddah, Saudi Arabia

***Corresponding Author**
Taimoor Shahid Malik
Consultant, Airport Special Systems, Jeddah, Saudi Arabia

Article History
Received: 27.06.2026
Accepted: 21.08.2026
Published: 24.08.2026

Abstract: Saudi Arabia's Vision 2030 and Saudi Aviation Strategy require airports to accommodate major growth while maintaining strong protection of passengers, aircraft, infrastructure, and digital systems. This review examines how artificial intelligence can strengthen airport security through intelligent video surveillance, automated baggage-screening support, biometric identity management, anomaly detection, cybersecurity analytics, predictive maintenance, and integrated command-and-control. It uses a structured narrative review of recent peer-reviewed literature and official aviation-policy sources. The analysis finds that AI can improve detection consistency, prioritise alarms, reduce equipment downtime, support passenger throughput, and enhance situational awareness. Nevertheless, airport security is a safety-critical domain in which false negatives, false positives, bias, privacy intrusion, cyberattack, model drift, and over-reliance on automation can create serious consequences. The paper proposes a five-layer Saudi framework covering data and sensing, AI analytics, operational response, governance and assurance, and Vision 2030 outcomes. It also recommends a phased implementation roadmap based on baseline assessment, controlled pilots, independent validation, workforce preparation, monitored scaling, and national coordination. The central conclusion is that AI should augment rather than replace aviation-security professionals. When deployed through human oversight, local validation, cybersecurity-by-design, transparent accountability, and continuous performance monitoring, AI-enabled security systems can support safe, smart, efficient, and globally competitive Saudi airports.

Keywords: Artificial Intelligence, Airport Security, Saudi Arabia, Vision 2030, Smart Airports, Aviation Security, Computer Vision, Predictive Maintenance, Cybersecurity.

1. INTRODUCTION

Saudi Arabia is undertaking one of the world's most ambitious aviation transformations. Under Vision 2030 and the Saudi Aviation Strategy, the Kingdom seeks to become a global aviation and logistics hub, expand airport capacity, improve the passenger experience, strengthen safety, and connect the country to more than 250 destinations. The strategy targets approximately 330 million passengers and 4.5 million tonnes of air cargo annually by 2030, placing substantial pressure on airport security systems to process higher volumes without weakening protection or creating excessive delays (General Authority of Civil Aviation [GACA], 2026a). This expansion is occurring alongside new airport developments, airline growth, smart gates,

automated baggage systems, and broader digital transformation across the transport sector (GACA, 2026b).

Airport security is a safety-critical and nationally significant activity. It includes passenger and baggage screening, access control, perimeter protection, video surveillance, explosives and narcotics trace detection, cybersecurity, identity verification, incident command, and the protection of airport communications and operational technology. Traditional security arrangements often depend on fixed rules, manual observation, isolated systems, and retrospective investigation. These approaches remain necessary, but they are increasingly challenged by high passenger volumes, complex threat patterns, insider risks, cyber-physical attacks, and the need to coordinate many agencies and technology platforms in real time.

Artificial intelligence (AI) can support this environment by analysing large and varied data streams faster than human operators, identifying subtle patterns, prioritising alarms, automating routine checks, and improving maintenance and resource allocation. Relevant techniques include computer vision, machine learning, deep learning, natural-language processing, biometric matching, anomaly detection, predictive analytics, and digital twins. In airport settings, these tools can assist with prohibited-item detection in X-ray images, unattended-object detection, behavioural anomaly identification, queue forecasting, access-control risk scoring, perimeter monitoring, and predictive maintenance of security equipment.

However, AI adoption in aviation security cannot be treated as a conventional information-technology upgrade. False negatives may permit a threat to pass undetected, while false positives can disrupt operations, increase passenger inconvenience, and overload security teams. Biometric and behavioural systems raise privacy, fairness, and data-governance concerns. AI models can also be attacked through manipulated inputs, data poisoning, model theft, or adversarial examples. Safety-critical research therefore emphasises explainability, verification, human oversight, robust engineering, and continuous monitoring rather than accuracy alone (Borg *et al*., 2021; Zhang *et al*., 2022).

This paper reviews the role of AI-enabled airport security systems in Saudi Arabia and proposes an implementation framework aligned with Vision 2030. It addresses four questions: (1) Which AI applications are most relevant to airport security? (2) How can these applications support Saudi aviation objectives? (3) What technical, organisational, ethical, and regulatory risks must be controlled? and (4) What phased roadmap can enable safe, scalable, and trustworthy deployment? The paper contributes a Saudi-focused synthesis linking airport-security technologies with national aviation goals, while retaining the human-centred and risk-based principles required for civil aviation security.

2. REVIEW METHODOLOGY

This study adopts a structured narrative-review approach. It combines peer-reviewed research on AI, computer vision, cybersecurity, biometrics, anomaly detection, explainable AI, and safety-critical systems with official Saudi and international aviation-policy sources. Literature was conceptually screened for relevance to airport security, operational reliability, real-time decision support, critical-infrastructure protection, and responsible AI. Priority was given to studies published from 2020 onward, while selected earlier works were retained where they provide foundational definitions or widely used technical approaches.

The review was organised into five analytical categories: sensing and data acquisition; AI-supported detection and prediction; operational response; governance and assurance; and Vision 2030 outcomes. This structure reflects the complete security cycle rather than treating an AI model as an isolated component. For example, a computer-vision model is operationally useful only when camera coverage, data quality, alarm thresholds, operator interfaces, escalation procedures, maintenance, cyber protection, and incident review are jointly designed.

The paper does not present experimental performance results or claim that a specific model has been validated at a Saudi airport. Instead, it synthesises published evidence and develops a conceptual framework for pilots, evaluation, and scaled implementation. This distinction is important because airport-security data are often restricted, threat prevalence differs by location, and model performance can degrade when operational conditions change. The recommendations therefore emphasise controlled trials, local validation, and governance before full deployment.

3. Saudi Aviation Transformation and Security Context

Vision 2030 positions transport, tourism, logistics, digital infrastructure, and public-sector effectiveness as key enablers of economic diversification. Aviation is central to these objectives because airports connect tourism destinations, pilgrimage flows, trade corridors, major projects, and international investment. GACA's aviation programme aims to improve safety, service quality,

airport infrastructure, operational processes, and environmental sustainability while expanding passenger and cargo capacity (GACA, 2026a). The scale of this ambition creates a direct security requirement: higher throughput must be achieved with equal or stronger protection.

Saudi airport environments are operationally diverse. They include large international hubs, pilgrimage gateways, domestic and regional airports, royal and VIP facilities, cargo terminals, and airports serving strategic projects. Security architectures commonly combine CCTV, access control, intrusion detection, X-ray screening, explosive trace detection, radio systems, fire and life-safety systems, passenger boarding bridges, baggage handling, building-management systems, and airport networks. The candidate profile that motivated this review reflects practical experience across many of these systems and across more than twenty-five Saudi airports, reinforcing the relevance of an integrated rather than device-specific research perspective.

Saudi Arabia's national civil aviation security programme is designed to protect airports, aircraft, passengers, cargo, and aviation-related shipments in alignment with international guidance, including ICAO standards (GACA, 2026c). ICAO's security framework requires states to prevent and respond to acts of unlawful interference, while its safety framework promotes risk management, state safety programmes, and safety-management systems. AI deployment should therefore complement existing regulatory controls, not replace them. The purpose is to improve situational awareness, consistency, speed, and resource prioritisation while preserving accountable human decision-making.

The Kingdom's digital transformation also increases exposure to cyber-physical risk. Modern screening devices, cameras, access systems, databases, and command platforms are networked and increasingly software-dependent. A disruption may begin as a cyber incident but create physical-security consequences, operational delays, or loss of public trust. Consequently, airport AI must be governed as part of critical national infrastructure. Security-by-design, network segmentation, identity and access management, secure updates, supplier assurance, logging, and resilience planning should be integrated from procurement through retirement.

A further contextual factor is passenger diversity. Saudi airports serve citizens, residents, pilgrims, tourists, business travellers, and transit passengers from many linguistic, cultural, and demographic groups. Biometric or behavioural models trained on narrow datasets may perform unevenly across these populations. Local evaluation must therefore examine subgroup performance, environmental conditions, clothing variations, crowd density, lighting, camera angle, and seasonal peaks. Responsible deployment requires evidence that systems are not only accurate in a laboratory but dependable and fair in the actual airport environment.

4. AI Applications in Airport Security

4.1 Intelligent Video Surveillance and Computer Vision

Video surveillance is one of the most mature areas for AI-assisted airport security. Computer-vision models can detect unattended baggage, entry into restricted zones, perimeter intrusion, crowd congestion, unusual movement, vehicle anomalies, or objects left in sensitive areas. Unlike conventional motion detection, deep-learning systems can classify objects and activities, allowing alarms to be prioritised according to context. At large Saudi airports, this capability could help operators manage thousands of camera streams and focus attention on events requiring verification.

The operational design must nevertheless prevent "automation bias," in which staff accept model outputs without sufficient challenge. AI should function as a decision-support layer. Alerts need confidence scores, location context, relevant video clips, and clear response procedures. Models should also be evaluated in conditions such as glare, dust, heat haze, low light, camera vibration, crowded pilgrimage operations, and partial occlusion. Explainable interfaces can improve operator trust by indicating the object, trajectory, or feature that triggered an alarm rather than presenting an unexplained risk label.

4.2 AI-Assisted Passenger and Baggage Screening

Security screening generates image-rich data suitable for machine learning. Convolutional neural networks and related architectures can assist operators by highlighting suspected weapons, explosives, prohibited items, or concealed components in cabin baggage and hold baggage images. Automated detection can reduce visual-search burden and support consistent decisions during peak periods. Similar methods may support trace-detection interpretation and multi-sensor fusion where X-ray, computed tomography, explosive trace detection, and passenger-risk information are considered together.

The main challenge is the extremely low tolerance for missed threats. Models trained on historical threat images may not recognise novel concealment methods or rare item configurations. Synthetic data and threat-image projection can

expand training coverage, but they should not substitute for realistic testing. Saudi deployment should use controlled operational trials, blind testing, and continuous comparison between AI-assisted and conventional screening outcomes. Human screeners must retain authority, and the system should be able to revert safely to manual operations.

4.3 Biometric Identity and Access Management

Biometric systems can strengthen passenger processing and staff access control by linking a person's identity to travel or employment credentials. Facial recognition, fingerprint, iris, and multimodal biometrics can support smart gates, employee authentication, and watch-list matching. When integrated correctly, biometrics may reduce document fraud and speed passenger movement, supporting the Vision 2030 objective of a seamless traveller experience.

Biometrics also create significant governance obligations. Templates are sensitive personal data, and breaches may have long-term consequences because biological characteristics cannot be changed like passwords. Systems must apply data minimisation, encryption, strict retention limits, access logging, and purpose limitation. Accuracy should be measured by false-match and false-non-match rates across relevant demographic groups. Decisions with serious consequences should require human verification and an accessible process for resolving identity errors.

4.4 Behavioural Analytics and Anomaly Detection

Machine learning can identify deviations from expected patterns in passenger movement, staff access, network use, or equipment behaviour. Examples include repeated access attempts, unusual movement between secure zones, an employee using systems outside normal duties, or a vehicle following an abnormal route. Deep-learning research on insider-threat detection shows potential for learning complex patterns from heterogeneous activity data, but also highlights data sparsity, limited labels, privacy concerns, and adaptive adversaries (Liu *et al*., 2021).

Behavioural analytics should therefore be used to prioritise review, not to infer criminal intent automatically. Many unusual actions have legitimate explanations. Models should be calibrated to minimise unnecessary intervention and should provide interpretable indicators such as "access outside assigned shift" or "movement inconsistent with authorised zone." Combining technical alerts with supervisory review, employment controls, and established security procedures is safer than relying on opaque behavioural scores.

4.5 Cybersecurity and Threat Intelligence

Airport security systems increasingly depend on digital networks, cloud services, software updates, and data exchange. AI can support cybersecurity by detecting anomalous traffic, malware behaviour, credential abuse, data exfiltration, or coordinated attacks. A major review of AI for cybersecurity found applications across identification, protection, detection, response, and recovery, while also identifying challenges related to data representation, evolving threats, and trustworthy infrastructure (Kaur *et al*., 2023).

For Saudi airports, cyber analytics should cover both enterprise IT and operational technology. Security-operation centres need visibility into cameras, access-control servers, baggage systems, screening equipment, radio networks, and third-party maintenance connections. Model alerts should integrate with incident-response playbooks and business-continuity plans. Because attackers may target the AI system itself, controls should include adversarial testing, secure model storage, validation of software updates, monitoring for data drift, and independent penetration testing.

4.6 Predictive Maintenance of Security Assets

AI-enabled predictive maintenance uses equipment data to estimate degradation and identify likely failures before they disrupt operations. Relevant inputs include fault codes, operating hours, temperature, vibration, image quality, power quality, network latency, alarm history, spare-parts consumption, and maintenance records. For airport security assets such as X-ray machines, CCTV cameras, access-control panels, UPS systems, and radio equipment, predictive maintenance can reduce downtime and improve availability.

This application directly supports safety and capacity. A screening lane that fails during a peak period can create queues, pressure, and security workarounds. Predictive analytics can help maintenance teams schedule intervention during low-demand periods, prioritise critical assets, and improve spare-parts planning. The greatest value arises when AI is integrated with a computerised maintenance-management system, asset criticality analysis, and service-level indicators. Predictions should be traceable to engineering evidence and reviewed by qualified maintenance personnel.

4.7 Integrated Command-And-Control and Decision Support

The highest strategic value may come from integrating multiple systems into a common operational picture. An AI-enabled security operations centre could correlate a door-forced alarm, nearby video, staff credential data, vehicle

movement, network anomalies, and relevant incident history. Instead of presenting operators with separate alarms, the platform can assemble an incident narrative and recommend response priorities.

Such integration must avoid creating a single point of failure. Architecture should be modular, resilient, and capable of degraded-mode operation. Data standards, time synchronisation, interoperability, and interface governance are essential. Recommendations should remain advisory unless the action is low risk and fully tested. High-consequence actions, such as denying travel, detaining a person, or closing a terminal area, require accountable human authorisation.

Table 1: Priority AI applications for Saudi airport security

Application	Primary data	Security value	Key control
Video analytics	CCTV and thermal video	Prioritises intrusion, unattended-object and crowd alerts	Human verification and local-condition testing
Screening assistance	X-ray/CT and trace-detection data	Highlights suspected prohibited items	Blind testing and safe manual fallback
Biometric identity	Face, iris or fingerprint templates	Strengthens identity and access assurance	Privacy, retention and demographic performance controls
Cyber anomaly detection	Network and system logs	Identifies suspicious digital activity	Adversarial testing and incident-response integration
Predictive maintenance	Fault codes, telemetry and CMMS records	Reduces security-equipment downtime	Engineering review and traceable recommendations

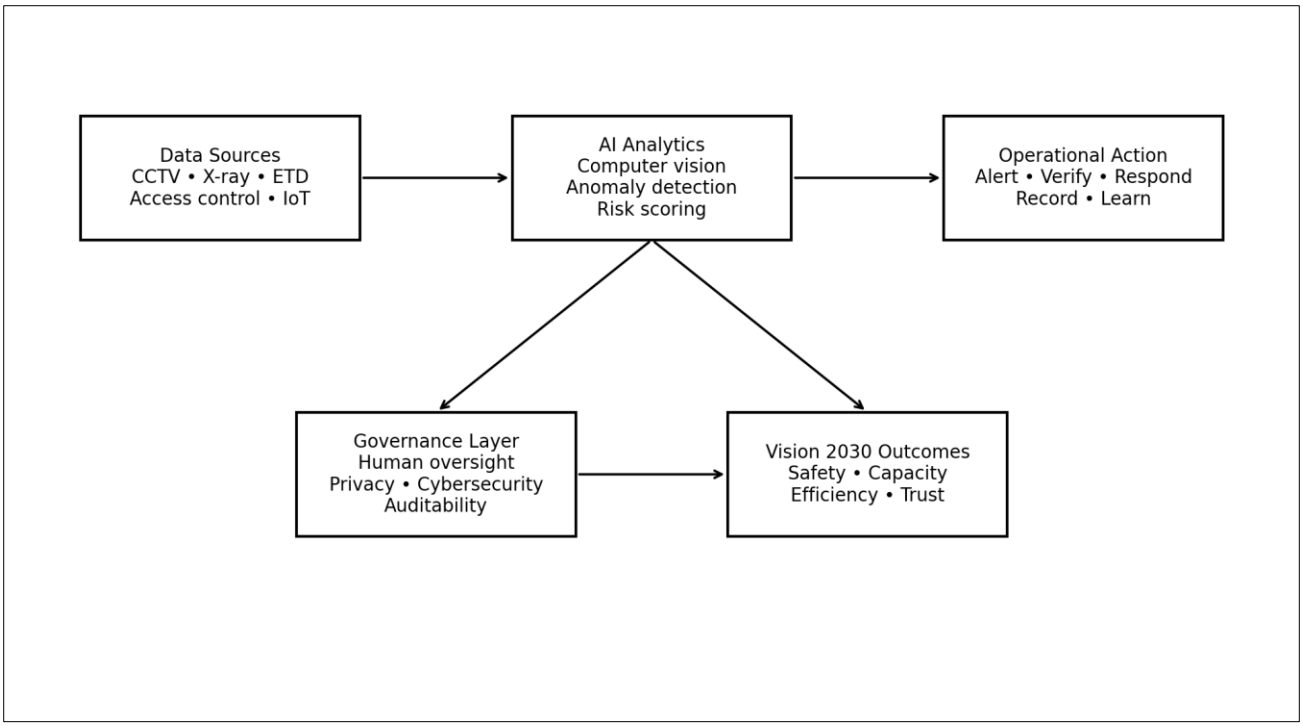

Figure 1: Integrated AI-enabled airport security framework

5. Vision 2030 Value Proposition

AI-enabled airport security can contribute to Vision 2030 through five connected outcomes. First, it can strengthen safety and security by improving detection consistency, correlating weak signals, and accelerating response. Second, it can support capacity growth by reducing bottlenecks and allowing security resources to be allocated according to demand and risk. Third, it can improve passenger experience through faster identity verification, more predictable queues, and fewer unnecessary secondary checks. Fourth, it can enhance operational efficiency through predictive maintenance, automated reporting, and better use of existing infrastructure. Fifth, it can build national capability in aviation technology, data science, cybersecurity, and systems engineering.

These benefits should be evaluated through balanced indicators. Detection performance is

necessary but insufficient. Airports should also measure false-alarm rates, operator workload, alarm-response time, system availability, passenger-processing time, privacy complaints, cybersecurity events, maintenance cost, energy use, and staff acceptance. A system that slightly improves detection but doubles false alarms may be operationally harmful. Conversely, a predictive-maintenance model that prevents critical downtime may create substantial security value even though it does not identify passengers or threats.

AI can also support localisation and workforce development. Saudi universities, technology companies, airports, regulators, and security organisations can collaborate on anonymised datasets, test environments, professional training, and applied research. This would help reduce dependence on imported "black box" solutions and allow systems to be adapted to local operating conditions. Procurement can encourage knowledge transfer, Arabic-language interfaces, local support, transparent performance evidence, and integration with national cybersecurity and data-governance requirements.

The overall value proposition is therefore not simply automation. It is the creation of a more anticipatory, evidence-driven, resilient, and passenger-centred security ecosystem. The human workforce remains central, but its role shifts from continuous low-value monitoring toward verification, investigation, coordination, and high-judgement decisions.

6. Risks, Constraints and Governance Requirements

6.1 Accuracy, Drift and Operational Validity

AI performance depends on the data and conditions under which a model was developed. Changes in camera placement, passenger composition, equipment software, lighting, threat behaviour, or operating procedures can reduce accuracy over time. Airports should establish model-performance baselines, drift indicators, revalidation schedules, and thresholds for suspension or rollback. Validation must use local data and realistic scenarios, including rare but high-consequence events.

6.2 Explainability and Human Factors

Security officers need to understand enough about an alert to take proportionate action. Explainable AI research argues that users require meaningful reasons for predictions, particularly in high-stakes environments (Minh *et al*., 2022). Explanations should be designed for the task rather than presented as technical visualisations that operators cannot interpret. Interfaces should show evidence, confidence, limitations, and recommended checks. Training must address automation bias, over-reliance, complacency, and the correct response when AI and human judgement disagree.

6.3 Bias, Privacy, and Proportionality

Biometric and behavioural systems may produce unequal error rates or intrusive monitoring. Governance should begin with a clear purpose and legal basis, followed by privacy-impact assessment, data minimisation, retention controls, role-based access, and independent audit. Not every available data source should be used. The proportionality question is whether the security benefit justifies the privacy impact and whether a less intrusive method could achieve the same result.

6.4 Cybersecurity and Adversarial Manipulation

Machine-learning systems introduce attack surfaces beyond conventional software. Attackers may manipulate sensor inputs, poison training data, steal model parameters, exploit dependencies, or create adversarial patterns that cause misclassification. Trustworthy-ML engineering recommends threat modelling, secure development, robustness testing, controlled access to training pipelines, provenance tracking, and monitoring after deployment (Zhang *et al*., 2022). Airport AI should be included in cybersecurity exercises and incident reporting rather than treated as a separate innovation project.

6.5 Interoperability and Legacy Infrastructure

Airports operate equipment from multiple vendors and generations. Proprietary interfaces can prevent data sharing or create expensive dependence on a single supplier. A scalable Saudi architecture should promote documented interfaces, data standards, modular procurement, and clear ownership of operational data. Integration projects must also account for latency, time synchronisation, network availability, and the consequences of partial system failure.

6.6 Regulation, Certification, and Accountability

Responsibility must remain clear when AI contributes to a security decision. Airports need defined roles for the regulator, airport operator, security provider, technology vendor, data controller, system integrator, and end user. Procurement contracts should specify performance, audit rights, cybersecurity obligations, update controls, incident notification, data ownership, and exit arrangements. High-risk applications should pass staged assurance gates before operational use.

6.7 Organisational Readiness and Change Management

Technology alone does not produce security improvement. AI programmes require senior

sponsorship, operational ownership, qualified data and engineering teams, user training, maintenance capacity, and a culture of incident learning. Staff may resist systems perceived as surveillance of employees or as a threat to employment. Communication should explain that AI is intended to augment professional judgement, improve safety, and reduce repetitive workload. Front-line operators should participate in design and evaluation.

Table 2: Principal risks and recommended controls

Risk	Potential consequence	Recommended control
False negative	Threat not detected	Conservative thresholds, multi-layer screening and blind validation
False positive	Delay, overload and passenger disruption	Contextual verification and workload monitoring
Model drift	Performance declines after deployment	Drift indicators, scheduled revalidation and rollback
Bias or privacy failure	Unequal treatment or loss of trust	Impact assessment, subgroup testing and data minimisation
Cyberattack on AI	Manipulated or unavailable security service	Secure development, adversarial testing and segmented architecture
Automation bias	Operator accepts incorrect output	Training, explainable alerts and retained human authority

7. Proposed Saudi AI-Enabled Airport Security Framework

The proposed framework consists of five layers. The first is the data and sensing layer, covering video, screening images, biometrics, access logs, perimeter sensors, equipment telemetry, network events, and operational databases. Data quality, time synchronisation, device health, and lawful collection are controlled at this layer.

The second is the analytics layer, where computer vision, anomaly detection, predictive models, identity matching, and data-fusion services generate alerts or forecasts. Models should be version-controlled, tested against defined scenarios, and monitored for drift. The third is the operational layer, which converts model outputs into verified actions through security officers, maintenance teams, supervisors, and incident commanders. It includes alarm prioritisation, standard operating procedures, escalation, communication, and fallback arrangements.

The fourth is the governance and assurance layer. It cuts across all technical components and includes cybersecurity, privacy, human oversight, safety assurance, ethics, procurement, audit, performance monitoring, and regulatory compliance. The fifth is the outcome layer, which evaluates contribution to Vision 2030 through safety, capacity, passenger experience, operational efficiency, resilience, and national capability.

A key principle is that each use case should have an explicit "human-AI decision contract." This contract identifies what the AI observes, what it predicts, how uncertainty is presented, who verifies the output, which actions are permitted, and how errors are recorded. For example, an unattended-bag model may be authorised to create an operator alert and display the relevant camera sequence, but not to trigger an evacuation automatically. A predictive-maintenance model may recommend inspection, while a licensed engineer decides whether equipment can remain in service.

Another principle is evidence proportionality. The stronger the consequence of a decision, the stronger the required validation, explainability, oversight, and appeal process. Low-consequence applications such as queue forecasting can be introduced more quickly. High-consequence applications such as watch-list matching, automated threat classification, or staff-risk scoring require stricter assurance.

8. Implementation Roadmap for Saudi Airports

Phase 1: Baseline assessment and use-case selection. Each airport should map existing security systems, threat scenarios, data availability, network architecture, maintenance performance, and operational pain points. Use cases should be ranked by security value, feasibility, privacy impact, integration complexity, and consequence of error. Predictive maintenance, video-event prioritisation, and queue forecasting may offer suitable early pilots because they can generate value without transferring final authority to an algorithm.

Phase 2: Controlled pilot and regulatory sandbox. Selected systems should be tested in a limited area or in shadow mode, where the AI produces outputs without controlling operations. Performance should be compared with current practice using agreed metrics. Pilots should include representative peak periods and environmental conditions, not only demonstration scenarios. Security, privacy,

cybersecurity, and human-factors reviews should occur before live use.

Phase 3: Validation and assurance. Independent teams should test accuracy, false alarms, resilience, subgroup performance, adversarial robustness, failover, data retention, and operator comprehension. Acceptance criteria must be established before testing. Any model update should trigger controlled revalidation. Documentation should include data sources, limitations, model version, test evidence, approved use, and rollback procedures.

Phase 4: Integration and workforce preparation. Approved AI services should be integrated with command centres, maintenance systems, identity platforms, and incident procedures. Operators and engineers need scenario-based training, including how to challenge an output and how to respond when the system is unavailable. Maintenance contracts should include model monitoring, secure updates, and technical support.

Phase 5: Scaled deployment and continuous monitoring. Expansion across terminals or airports should occur only after benefits are demonstrated. A central assurance function can maintain common standards while allowing local adaptation. Performance dashboards should combine technical, operational, security, privacy, and passenger indicators. Incidents and near misses should feed back into model and procedure improvement.

National coordination can accelerate this roadmap. GACA, airport operators, cybersecurity authorities, universities, and industry partners could establish shared evaluation protocols, secure test datasets, professional competencies, and reference architectures. A national aviation-security AI laboratory or sandbox would allow vendors and researchers to test systems against Saudi-relevant conditions without exposing live operational networks.

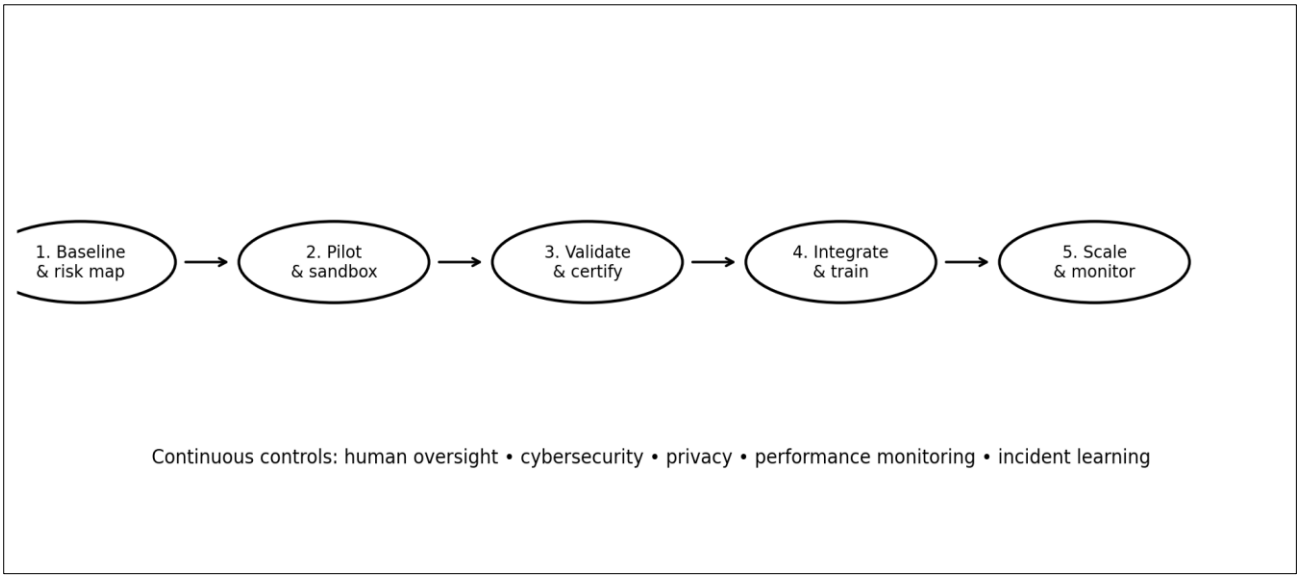

Figure 2: Phased implementation roadmap for Saudi airports

9. DISCUSSION

The review indicates that AI can materially strengthen Saudi airport security, but its greatest value lies in augmentation and integration rather than full autonomy. Airports already possess extensive sensors and systems; the challenge is converting fragmented data into timely, reliable, and accountable decisions. AI can help operators recognise patterns that would be difficult to detect manually, while predictive analytics can improve the availability of critical assets.

The strongest near-term opportunities are likely to be applications with measurable operational benefits and controlled consequences: predictive maintenance, intelligent video-event filtering, cybersecurity anomaly detection, and passenger-flow forecasting. These use cases can build organisational capability and trust before more sensitive applications are scaled. Automated threat detection and biometrics may provide major benefits, but they require stronger validation and governance because errors directly affect security and individual rights.

Saudi Arabia has advantages for responsible deployment. Major airport investments create opportunities to design digital and security architecture from the outset rather than retrofitting every component. National strategies provide clear performance goals, and the Kingdom can coordinate regulators, operators, technology providers, and research institutions. At the same time, rapid expansion creates the risk of fragmented pilots,

vendor lock-in, or technology adoption driven by novelty rather than operational need. A common assurance framework would reduce these risks.

The paper's proposed framework links technical capability to operational action and national outcomes. This is necessary because model-level metrics can be misleading. A high-performing classifier may fail to improve security if alarms are poorly displayed, staff are not trained, or integration creates delays. Conversely, a modestly complex model may deliver significant value if it prevents equipment failures or reduces operator overload. Evaluation should therefore focus on system performance and security outcomes, not algorithm accuracy alone.

There is also a research opportunity to develop Saudi-specific evidence. Future studies could evaluate AI-assisted screening under local passenger and environmental conditions, compare predictive-maintenance methods across airport assets, examine operator trust and workload, measure the effectiveness of explainable alerts, and assess privacy-preserving approaches to biometric and behavioural analytics. Research partnerships could use anonymisation, federated learning, synthetic data, and secure research environments to address the sensitivity of aviation-security data.

Finally, AI should be understood as part of a broader smart-airport transformation. Security systems interact with passenger processing, facility management, emergency response, airlines, ground handling, customs, border control, and cybersecurity. Integrated governance is essential so that improvements in one area do not create vulnerabilities elsewhere. Vision 2030 provides a strategic reason to pursue innovation, but aviation-security principles require that innovation remain risk-based, human-centred, and demonstrably safe.

10. CONCLUSION

Artificial intelligence can support Saudi Arabia's ambition to build safe, smart, efficient, and globally competitive airports under Vision 2030. Applications in computer vision, screening, biometrics, anomaly detection, cybersecurity, predictive maintenance, and integrated command-and-control can improve detection, accelerate response, reduce downtime, and support growing passenger and cargo volumes.

The benefits are not automatic. Airport AI operates in a safety-critical, security-sensitive, and privacy-intensive environment. Systems must be locally validated, explainable to users, resilient to cyberattack, monitored for performance drift, and governed through clear human accountability. High-consequence decisions should remain subject to qualified human verification.

A phased approach—baseline assessment, controlled pilot, independent validation, integration and training, followed by monitored scaling—offers the most credible path. Saudi stakeholders can strengthen this process through common standards, national test environments, secure research partnerships, and procurement requirements that support interoperability and knowledge transfer.

The central recommendation is to treat AI not as a replacement for aviation-security professionals but as an intelligence and assurance layer that improves their ability to protect passengers, infrastructure, and operations. When deployed within a strong governance framework, AI-enabled security can become an important enabler of the Saudi Aviation Strategy and a practical contribution to Vision 2030.

REFERENCES

- Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data, 8, 53. https://doi.org/10.1186/s40537-021-00444-8
- Borg, M., Englund, C., Wnuk, K., Duran, B., Levandowski, C., Gao, S., Tan, Y., Kaijser, H., Lönn, H., & Törngren, M. (2021). Safely entering the deep: A review of verification and validation for machine learning and a challenge elicitation in the automotive industry. Journal of Automotive Software Engineering, 1(1), 1-19.
- Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv:1702.08608.
- European Union Aviation Safety Agency. (2023). Artificial Intelligence Roadmap 2.0: A human-centric approach to AI in aviation. EASA.
- General Authority of Civil Aviation. (2026a). Saudi Aviation Strategy. Government of Saudi Arabia.
- General Authority of Civil Aviation. (2026b). Saudi 2030 elevates aviation: King Salman Airport, advanced air mobility and sustainable innovation. Government of Saudi Arabia.
- General Authority of Civil Aviation. (2026c). National programmes for civil aviation security. Government of Saudi Arabia.
- International Civil Aviation Organization. (2022). Global Aviation Safety Plan 2023-2025. ICAO.
- International Civil Aviation Organization. (2024). Aviation security: Reporting of acts of unlawful interference. ICAO.

- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
- Liu, L., De Vel, O., Han, Q.-L., Zhang, J., & Xiang, Y. (2021). Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys & Tutorials, 20(2), 1397-1417.
- Madan, R., & Ashok, M. (2023). AI adoption and diffusion in public administration: A systematic literature review and future research agenda. Government Information Quarterly, 40(1), 101774. https://doi.org/10.1016/j.giq.2022.101774
- Minh, D., Wang, H. X., Li, Y. F., & Nguyen, T. N. (2022). Explainable artificial intelligence: A comprehensive review. Artificial Intelligence Review, 55, 3503-3568. https://doi.org/10.1007/s10462-021-10088-y
- Mohseni, S., Zarei, N., & Ragan, E. D. (2021). A multidisciplinary survey and framework for design and evaluation of explainable AI systems. ACM Transactions on Interactive Intelligent Systems, 11(3-4), 1-45. https://doi.org/10.1145/3387166
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
- Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence. OECD.
- Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1, 206-215. https://doi.org/10.1038/s42256-019-0048-x
- Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2, 160. https://doi.org/10.1007/s42979-021-00592-x
- Shneiderman, B. (2022). Human-Centered AI. Oxford University Press.
- Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology.
- Tjoa, E., & Guan, C. (2021). A survey on explainable artificial intelligence (XAI): Toward medical XAI. IEEE Transactions on Neural Networks and Learning Systems, 32(11), 4793-4813. https://doi.org/10.1109/TNNLS.2020.3027314
- United Nations Educational, Scientific and Cultural Organization. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.
- Wang, Y., Zhang, H., & Wu, Q. (2023). Identifying and managing risks of AI-driven operations: A case study of automatic speech recognition for improving air traffic safety. Chinese Journal of Aeronautics, 36(4), 366-386. https://doi.org/10.1016/j.cja.2022.08.020
- Zhang, J. M., Harman, M., Ma, L., & Liu, Y. (2022). Machine learning testing: Survey, landscapes and horizons. IEEE Transactions on Software Engineering, 48(1), 1-36. https://doi.org/10.1109/TSE.2019.2962027
- Zhou, J., Gandomi, A. H., Chen, F., & Holzinger, A. (2021). Evaluating the quality of machine learning explanations: A survey on methods and metrics. Electronics, 10(5), 593. https://doi.org/10.3390/electronics10050593.