

شناسایی و اولویت‌بندی راهکارهای ارتقای امنیت فرودگاه‌ها مبتنی بر فناوری‌های نوین

عبدالعلی جلالی^۱

حمیدرضا ضرغامی^۲

علیرضا صابری^۳

چکیده:

امنیت فرودگاه از جنبه‌های مختلف برای دولت‌ها حائز اهمیت است. فرودگاه یکی از ستون‌های اصلی صنعت هوانوردی است و بیشترین تأثیر مستقیم را بر اقتصاد حمل‌ونقل هوایی دارد و نشان‌دهنده رشد اقتصادی، فرهنگی و میزان رفاه یک کشور است. با توجه به مداخله‌های غیرقانونی گسترده و چالش‌های امنیتی فرودگاه‌ها، بررسی طرح‌ها و تدابیر مختلف، برای ارتقای امنیت فرودگاه‌ها مبتنی بر فناوری‌های نوین لازم و ضروری است. در این پژوهش به شناسایی و اولویت‌بندی راهکارهای ارتقای امنیت فرودگاه‌ها با استفاده از فناوری‌های نوین پرداخته شده است. روش پژوهش به این صورت است که ابتدا با مطالعات اسناد و ضمایم سازمان بین‌المللی هواپیمایی کشوری و مرور مبانی نظری و پیشینه، چالش‌ها و راهکارهای موجود شناسایی و سپس با کمک روش توصیفی-پیمایشی مبتنی بر نظرات خبرگان دانشگاهی و صنعت هوانوردی به شناسایی و اولویت‌بندی راهکارهای شناسایی شده، پرداخته شد. ابزار اصلی گردآوری داده‌ها پرسش‌نامه است. روایی پرسش‌نامه با استفاده از روایی محتوایی و صوری و نیز پایایی آن از طریق آلفای کرونباخ مقدار ۰/۸۷ محاسبه و تأیید شده است. ابزار تحلیل داده‌ها نرم‌افزار EXCEL و SPSS است. با توجه به نرمال نبودن داده‌ها در بخش تحلیل استنباطی از آزمون‌های آماری ناپارامتریک (آزمون دوجمله‌ای) و برای بررسی تفاوت اولویت متغیرها از آزمون فریدمن استفاده شد. نتایج پژوهش راهکارهای مهم و اولویت‌دار این عرصه را مشخص کرد. بر این مبنا، مهم‌ترین راهکار شناسایی شده، فناوری تشخیص چهره برای تأیید هویت افراد و مهم‌ترین چالش امنیت فرودگاه‌ها تغییر در سبک و روش تروریست‌ها است. اولویت‌بندی راهکارها می‌تواند معیارهایی برای تصمیم‌گیری مدیران ارشد امنیتی فرودگاه‌ها باشد.

واژه‌های کلیدی: امنیت، مداخله غیرقانونی، فناوری‌های نوین، فرودگاه

aaajalali@gmail.com
Zarghami@jusst.ac.ir
saberialireza680@gmail.com

۱. استادیار مهندسی هوافضا دانشگاه علوم و فنون هوایی شهید ستاری
۲. استادیار مهندسی صنایع دانشگاه علوم و فنون هوایی شهید ستاری
۳. کارشناس ارشد عملیات هوانوردی دانشگاه علوم و فنون هوایی شهید ستاری

مقدمه

رشد ترافیک هوایی باعث گسترش و توسعه فرودگاه‌ها شده است. این رشد ناشی از افزایش تعداد مسافرها، بار همراه آن‌ها و محموله‌های است که به‌صورت هوایی جابجا می‌شود. برای جلوگیری از ورود اشیا غیرمجاز و یا افراد خطرناک به مناطق محدودشده فرودگاه نیاز به نظارت و بازرسی دقیق است؛ زیرا که کارکنان امنیتی با خطرهای نظیر حمله‌های تروریستی، اخلال یا تخریب تأسیسات فرودگاهی و آسیب به مسافران و استفاده از تجهیزات ممنوعه در فرودگاه‌ها برای انجام کارهای خرابکارانه روبه‌رو هستند. نظارت و بازرسی توسط کارکنان امنیتی زمان‌بر است و این باعث اتلاف وقت مسافران در پشت دروازه‌های امنیتی برای بازرسی بدنی و امنیتی شده و درنهایت باعث نارضایتی مسافران می‌شود.

بمب‌گذاری فرودگاه بروکسل در فوریه ۲۰۱۶ و حمله به فرودگاه آتاتورک در استانبول در ژوئن ۲۰۱۶ شواهدی از تاکتیک‌های در حال تحول تروریست‌ها برای حمله به مناطق آسیب‌پذیر به شیوه‌ای خاص است (Stewart & Mueller, 2014). در سال ۲۰۱۵، شرکت هواپیمایی لهستانی (LOT)، با یک حمله سایبری مواجه شد که حداقل ۲۲ پرواز با تأخیر و یا لغو روبه‌رو شدند؛ زیرا خلبان‌ها در هواپیما نمی‌توانستند دستورالعمل‌های برخاست را دریافت کنند. (Kagalwalla & Churi, 2019)

مطالعه‌ها حاکی از این دارد که در کنار استانداردها و قوانین بین‌المللی موجود، استفاده از فناوری نوین در راستای ارتقای امنیت فرودگاه‌ها، با توجه به گستردگی فرودگاه‌ها لازم و ضروری است؛ چراکه در این شرایط نیاز به تعداد بیشتری از کارکنان حفاظتی احساس می‌شود، از طرفی خستگی ناشی از افزایش کار سبب کاهش بازدهی و یا بروز رفتار ناشایست و یا در فرایند بازرسی امنیتی، مسافران با کارکنان غربالگری ارتباط برقرار می‌کنند، درنتیجه زمان نظارت و بازرسی افزایش پیدا می‌کند و باعث اتلاف وقت مسافران می‌شود (Kirschenbaum, 2013)؛ بنابراین به کارگیری فناوری‌های نوین برای ارتقای امنیت فرودگاه‌ها باعث کاهش خطای انسانی و استفاده از تعداد نیروی کار کمتری و مدیریت زمان و درنهایت رضایت مسافران می‌گردد.

ضمیمه ۱۷ سازمان بین‌المللی هواپیمایی کشوری (ICAO)^۱، یکی از ضمایم پیمان شیکاگو (۱۹۴۴) است. درواقع مهم‌ترین سند ایکائو در مورد امنیت هوانوردی است. در سال ۱۹۷۴ شورای ایکائو ضمیمه ۱۷ را تصویب نمود که موجب ادغام برخی از تعهدات مقرر در کنوانسیون‌های توکیو، لاهه و مونترال در این ضمیمه گردید. در این قسمت تعاریف طبق ضمیمه ۱۷ سازمان بین‌المللی هوانوردی کشوری و در ادامه استانداردهای پیمان شیکاگو مربوط به امنیت فرودگاه‌ها بیان می‌شود.

امنیت: حفاظت از هواپیمایی کشوری در مقابل رفتارهای مداخله غیرقانونی است که این هدف، به‌وسیله مجموعه‌ای از مقررات و منابع مادی و انسانی حاصل می‌شود. (ICAO, Annex 17, 2020)

1. Annex

2. international civil aviation organization

رفتارهای مداخله غیرقانونی: اعمالی که امنیت هواپیمایی کشوری و حمل‌ونقل هوایی را با خطر روبه‌رو کند، مانند تصرف غیرقانونی هواپیمای در حال پرواز یا بر روی زمین، گروگان‌گیری در هواپیما و یا در فرودگاه، نفوذ اجباری به هواپیما و یا به یک فرودگاه، انتقال سلاح و اشیاء خطرناک به هواپیما و یا فرودگاه به‌قصد ارتکاب اعمال جنایی، انتقال اطلاعات نادرست به طریقی که امنیت هواپیمای در حال پرواز و یا بر روی زمین، مسافرها، خدمه، کارکنان زمینی و یا مردم عادی در فرودگاه را به مخاطره اندازد. منطقه امنیتی محدودشده^۱: قسمت‌های از محدوده فرودگاه که به‌عنوان بخش‌های دارای اولویت خطر شناسایی می‌شوند. مکان‌های که علاوه بر کنترل دسترسی، کنترل امنیتی هم اعمال می‌شود. شامل تمام قسمت‌های خروج مسافر از نقطه نظارت تا هواپیما، باند، قسمت بسته‌بندی بار، محل سرویس هواپیما، نظارت بر چمدان و بار، محموله بار، مرکز نامه، تهیه و بسته‌بندی مواد غذایی و محدوده تمیزکاری هواپیما است. نظارت^۲ (غربالگری): استفاده از وسایل فنی یا موارد دیگر به‌منظور شناسایی، کشف اسلحه، مواد منفجره، وسایل خطرناک، اشیاء یا موادی که ممکن است، برای رفتارهای مداخله غیرقانونی استفاده شود. کنترل امنیتی^۳: مفهومی برای تشخیص بمب، مواد منفجره یا هرگونه وسیله، اشیاء و مواد خطرناک که برای رفتارهای مداخله غیرقانونی داخل هواپیما بکار می‌رود و باید از ورود آن به هواپیما جلوگیری شود. بازبینی امنیتی^۴: ارزیابی نحوه اجرای نیازمندی‌های برنامه ملی امنیت هوانوردی کشوری که توسط یک شرکت هواپیمایی، فرودگاه و یا سایر نهادهای درگیر با امور امنیتی باید اجرا شود. فرودگاه: منطقه‌ای بر روی زمین یا آب (شامل کلیه ساختمان‌ها، تأسیسات و تجهیزات نصب‌شده) است که از کل یا بخشی از آن‌ها برای ورود، خروج و جابجایی زمینی انواع وسایل پرنده و تسهیلات بار و مسافر مشخص استفاده می‌گردد.

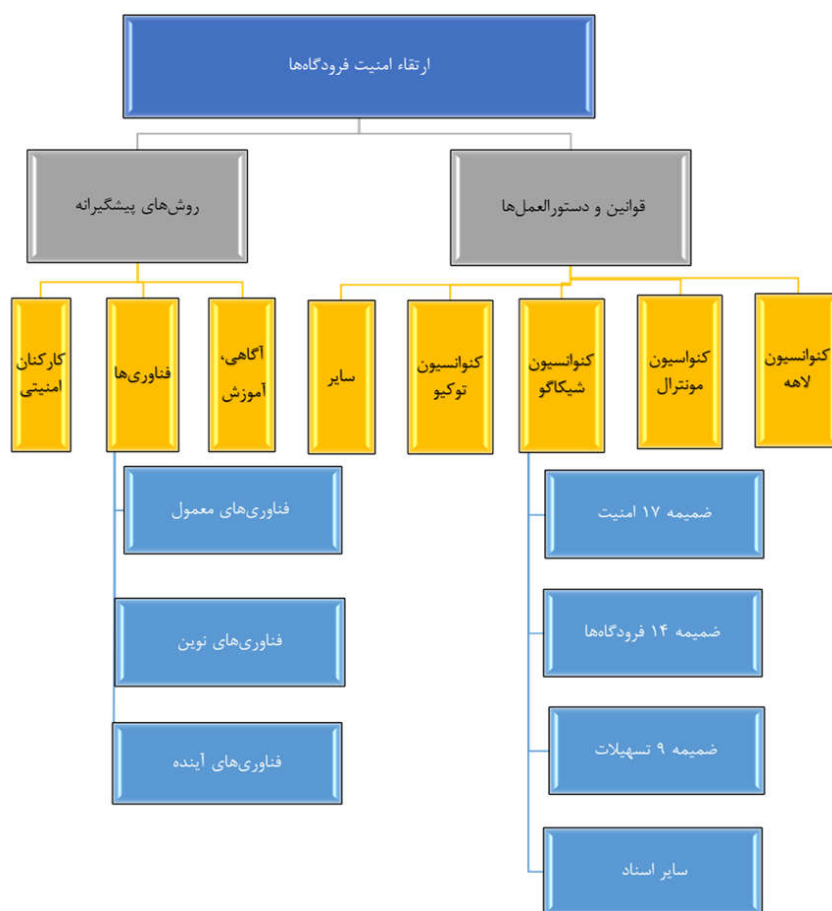
(ICAO, Annex 14, 2018)

ضمیمه ۹ پیمان شیکاگو که مربوط به تسهیلات فرودگاهی است و بیشترین توجه را به استفاده از فناوری‌های نوین در خصوص امنیت هوانوردی دارد و دولت‌های متعاهد را ملزم به معرفی یک سامانه اطلاعات پیشرفته مسافر و پیشنهاد استفاده از فناوری زیست‌سنج با تصویر عکس دیجیتال و اثرانگشت یا اسکن عنبر به‌صورت اختیاری که قابلیت خوانش ماشین را داشته باشد، در ادامه دولت‌ها را ملزم به بررسی و ارزیابی اسناد مسافر برای جلوگیری از جعل و سوءاستفاده و ورود افراد غیرمجاز به هواپیما می‌کند. (ICAO, Annex9, 2017)

فصل سه و نه جلد یک ضمیمه ۱۴ پیمان شیکاگو در مورد امنیت فرودگاه است. در فصل سه اشاره به ویژگی‌های فیزیکی فرودگاه مثل قرارگیری محل پارکینگ ایزوله (جداکننده) برای هواپیمایی که با رفتارهای

1. Security restricted area
2. Screening
3. Security search
4. Security inspection

مداخله غیرقانونی مانند بمب‌گذاری روبه‌رو شده می‌پردازد. در فصل نهم به طرح‌های اضطراری فرودگاه در موقعیت رفتارهای مداخله غیرقانونی و همچنین طرح حصار کشی و روشنایی از دید امنیتی اشاره شده است. در این ضمیمه در مورد موانع فرودگاهی برای جلوگیری از رفتارهای مداخله غیرقانونی و در بخش دیگر به جانمایی تأسیسات فرودگاه و محل قرارگیری پارکینگ‌های جداکننده هواپیماهایی که در معرض بمب‌گذاری و یا سایر مداخلات غیرقانونی قرار گرفته‌اند، می‌پردازد. شکل ۱ ارتقای امنیت فرودگاه‌ها را از دو دیدگاه رعایت قوانین و دستورالعمل‌های بین‌المللی و روش‌های پیشگیرانه نشان می‌دهد.



شکل ۱- راهکارهای ارتقای امنیت فرودگاه‌ها

اقدامات امنیتی پیشگیرانه

بر اساس ضمیمه ۱۷ سازمان بین‌المللی هواپیمایی کشوری هر دولت متعهد باید سنجش‌هایی را ایجاد

نماید تا از ورود اسلحه، بمب، مواد منفجره یا هرگونه وسیله، اشیا و مواد خطرناک که برای رفتارهای مداخله غیرقانونی به کار می‌رود، جلوگیری شود که این سنجش‌ها شامل موارد زیر است.

➤ اقدامات مرتبط با کنترل دسترسی

هر دولت متعهد باید موارد زیر را تضمین نماید:

- باید کنترل دسترسی به قسمت‌های خدماتی فرودگاه برای جلوگیری از ورود بدون مجوز انجام شود.
- سامانه‌های شناسایی با توجه به اشخاص و وسایل نقلیه به‌منظور جلوگیری به قسمت‌های مختلف فرودگاهی و مناطق محدودشده امنیتی ایجاد گردد و هویت در نقاط کنترل قبل از اجازه دسترسی به این مناطق، تأیید شود.
- بررسی‌های سوابق افراد غیر مسافر که اجازه دسترسی بدون همراه به مناطق محدودشده امنیتی در فرودگاه را دارند، قبل از مجوز دسترسی، انجام شود.

➤ اقدامات مرتبط به مسافران و بار درون کابین^۱ آنها

هر دولت متعهد باید موارد زیر را اطمینان دهد:

- سنجش‌های را ایجاد کند که مسافر و بارهای درون کابین آنها قبل از سوارشدن به هواپیما در حال خارج شدن از مناطق محدودشده امنیتی بررسی گردد.
- مسافران و بارهای درون کابین آنها که بررسی شده‌اند باید از مداخله بدون مجوز از نقطه نظارت تا زمان سوارشدن محافظت شوند. در صورت مخلوط شدن یا برقراری تماس مسافران و بارهای درون کابین آنها باید قبل از سوارشدن به هواپیما بازرسی مجدد انجام گردد.
- فرودگاه باید سنجش‌های را برای عملیات جابجایی بار درون کابین مسافران ایجاد کند تا از مداخله بدون مجوز محافظت شوند.

چالش‌های امنیت فرودگاه‌ها

تقریباً ۳۵۰ حمله تروریستی به فرودگاه‌ها یا هواپیماها بین سال‌های ۲۰۰۰ تا ۲۰۱۵ رخ داده است. (پایگاه داده جهانی تروریسم دانشگاه مریلند). استوارت و مولر در مقاله خود تهدیدهای امنیت فرودگاه را در چهار طبقه خودروهای بمب‌گذاری شده بزرگ، خودروهای بمب‌گذاری شده در کنار جاده، بمب جاگذاری شده در چمدان یا جلیقه و تیراندازی در اماکن عمومی فرودگاه‌ها ارزیابی می‌کنند. حمله‌ها به فرودگاه‌ها در چند سال گذشته بسیار مرگبار بوده است، مانند حمله به فرودگاه‌های بروکسل، ترکیه و فلوریدا را می‌توان نام برد. هواپیماها قبلاً منبع اصلی حمله‌ها بوده‌اند؛ اما اکنون هدف به سمت فرودگاه تغییر پیدا کرده است. (Bolton, 2017)

1. Cabin baggage

➤ چالش افزایش حجم ترافیک هوایی

طبق آمار سازمان بین‌المللی هواپیمایی کشوری در سال ۲۰۱۶، از سال ۱۹۷۷ رشد ترافیک هوایی هر پانزده سال دو برابر شده است. بر اساس پیش‌بینی بازار ایرباس (Airbus GMF 2018) در بیست سال آینده سالانه رشد ترافیک هوایی، ۴/۴ درصد است که در ده سال اول ۴/۸ و در ده سال دوم میانگین ۴ درصد و حدود ۳۷۴۰۰ فروند هواپیمای تجاری در ۲۰ سال آینده نیاز است؛ بنابراین، برای کنترل و نظارت امنیتی دقیق‌تر و سریع‌تر نیاز به استفاده از فناوری‌های نوین است.

➤ چالش افزایش مسافر و بار همراه

برای مسافران و هر نوع اقلام باید بررسی و نظارت امنیتی به‌طور متفاوتی انجام شود و چمدان‌های چک شده از مسیری جابجا شوند که مواد خاص، مواد منفجره و اشیاء ممنوعه شناسایی شوند.

➤ چالش افزایش محموله هوایی

محموله هوایی شامل چمدان‌های نزد مسافران در پرواز، بارهای مسافر که در شکم هواپیما و بارهای اختصاصی می‌شود. اجرای نظارت و بازرسی محموله‌ها در شکم هواپیماها زمان بیشتری از غربال‌گری مسافران می‌برد. مشکلاتی هم وجود دارد، به‌عنوان مثال، غربال‌گری بار هوایی در آخرین لحظه برای سوار کردن به هواپیما امکان‌پذیر نیست، چون که بارها در کانتینر یا جعبه است. در سال ۲۰۱۲ تروریست‌ها تلاش می‌کردند کارتریج‌های چاپگر را از یمن به ایالات متحده ارسال کنند که حاوی مواد منفجره بودند. (Karoly, 2017)

➤ چالش تمرکز شلوغی در یک نقطه خاص

تجمع تعداد قابل‌توجهی از مسافران در دهلیزها و دروازه‌های امنیتی، منطقه‌ای آشکار برای حمله تروریست‌ها است. گزارش شرکت RAND برافزایش بازدهی با اتخاذ اقداماتی برای کاهش تعداد افرادی که در صف‌های طولانی ایستاده‌اند، تمرکز دارد.

➤ چالش حساسیت بالای خبری و رسانه‌ای

فرودگاه‌ها برای رسانه‌های خبری مهم هستند؛ زیرا آن‌ها یک محل تجارت هستند و برای فعالیت به اعتماد عمومی متکی هستند.

➤ چالش پیچیدگی تهدیدها با توجه به رشد فناوری‌ها

با ورود فناوری‌های امنیتی جدید به فرودگاه‌ها، پیچیدگی تهدیدهای که کاربرهای فرودگاه با آن مواجه هستند نیز بیشتر شده است. در بمب‌گذاری فرودگاه بروکسل در فوریه ۲۰۱۶ و حمله به فرودگاه آتاتورک در استانبول در ژوئن ۲۰۱۶ شواهدی از تاکتیک‌های در حال تحول تروریست‌ها برای حمله به مناطق آسیب‌پذیر فرودگاه به شیوه‌ای خاص وجود داشت.

➤ چالش تغییر در سبک و روش تروریست‌ها

«استیو کارولی» معاون سرپرست دفتر تحلیل نیازمندی‌های اداره امنیت حمل‌ونقل ایالات متحده آمریکا بیان می‌کند: که امروزه تروریست‌ها در نحوه ساخت و کنترل بمب‌ها خلاق شده‌اند و از فضای باز و سترن نهایت استفاده را می‌برند. تروریست‌ها امروز بدون هیچ شرمی به‌طور عادی تمایل خود برای حمله به اهداف غیرنظامی هوانوردی و زیرساخت‌های هوانوردی را در رسانه‌های اجتماعی و تبلیغاتی پخش می‌کنند، به لطف اینترنت و سهولت تبادل اطلاعات و دانش در این فضا، تروریست‌های امروزی به راحتی می‌توانند دانش فنی را به اشتراک بگذارند.

➤ چالش هزینه‌های امنیتی

یک مشکل اساسی و زیربنایی، تأمین هزینه مالی امنیت فرودگاه‌ها است. چگونه می‌توان منابع کمیاب را به بهترین نحو تخصیص داد تا احتمال حمله موفقیت‌آمیز علیه فرودگاه‌ها به یک سطح پذیرفتنی کاهش یابد (Gillen & Morrison, 2015) نتایج جالب به دست آمده از پژوهش‌های انجام شده در این حوزه، نشان می‌دهد که حذف یا کوچک کردن لایه‌های امنیتی موجود به عنوان لایه‌های فناوری‌های جدید (Jackson & LaTourrette, 2015) و ارائه یک الگو و یک سامانه رایانه‌ای که توانایی در نظر گرفتن عوامل انسانی در روند غربالگری را داشته باشد (Skorupski & Uchroński, 2018) کمک شایانی به کاهش هزینه‌های امنیتی می‌کند.

➤ چالش بمب‌های دست‌ساز^۱

درگذشته، استانداردهای صدور گواهینامه برای سامانه‌های کشف مواد منفجره شامل چند ماده شیمیایی می‌شد که همه آن‌ها مواد منفجره تجاری و نظامی بودند. تهدید مواد منفجره مایع و مواد منفجره خانگی بعدها به این چالش‌های امنیتی اضافه گردید. مشکل مهم دستگاه‌های امنیتی طیف وسیع مواد منفجره تجاری، نظامی و خانگی است که در تقسیم‌بندی زیادی و در ابعاد گوناگون ارائه می‌شوند. از آنجایی که دشمن تمایل به اقدامات شدید برای حمله‌های خود دارد، از «دستگاه‌های مواد منفجره دست‌ساز انسان»^۲ که رایج‌تر و خطرناک‌تر هستند، استفاده می‌کند. (Karoly, 2017) این مواد منفجره را می‌توان به خوبی پنهان کرد. کشف بمب‌گذاری شده در سال ۲۰۰۱، لباس‌زیر بمب‌گذاری در سال ۲۰۰۹، جلیقه‌های انتحاری که مهاجم‌ها در فرودگاه بروکسل و استانبول (۲۰۱۶) پوشیده بودند نمونه‌ای از این موارد هستند.

➤ چالش تهدید پرنده‌های بدون سرنشین^۳

پرنده‌های بدون سرنشین خطر جدی برای زیرساخت‌های حیاتی فرودگاه‌ها هستند که می‌توانند مواد

1. (HME) Home Made Explosives

2. (PBIED) person-borne improvised explosive devices

3. (UAV) Unmanned Aerial Vehicle

منفجره و حتی راکت را با خود حمل کنند. از پمپاها می‌توان برای حملات سایبری به فرودگاه استفاده کرد. شناسایی پمپاها و خلبان کنترل‌کننده آن کار سختی است. در ایالات متحده، اداره هوانوردی فدرال^۱ و اداره کل ملی هوانوردی و فضا^۲، پایگاه اطلاعاتی دارند که تهدیدهای پرنده‌های بدون سرنشین را نگهداری و منتشر می‌کنند. چنین پایگاه داده‌ای برای شناسایی خطرات پمپاها بسیار مفید است. (Pyrgies, 2019)

➤ چالش تهدیدهای نوین امنیتی

تهدیدهای نوین امنیتی مانند تهدیدهای زیست‌محیطی، الکترومغناطیسی و سایبری چالش‌های جدید و نوظهور برای فرودگاه‌ها هستند.

➤ تهدیدهای سایبری

نرم‌افزارها و سخت‌افزارها به‌صورت گسترده در فرودگاه‌ها با تهدیدهای مجازی دست‌وپنجه نرم می‌کند. با استفاده از بدافزارها، نرم‌افزارهای مخرب و نفوذگرها، سامانه‌های اطلاعاتی کلیه بخش‌های هوانوردی شامل تجهیزات فرودگاه‌ها و هواپیماها در معرض خطر است.

ویژگی تروریسم مجازی گمنام بودن آن است که این امکان را برای نفوذگر ایجاد می‌کند تا نقاط بازرسی مثل محل‌های نظارت و یا هرگونه نشانه فیزیکی برای ردیابی را از میان ببرد. این نوع تروریسم دارای هزینه‌های اندک بوده که تنها هزینه‌هایی را که برای اختلال در برنامه‌های رایانه‌ای یک نظام حمل‌ونقل هوایی به بار می‌آورد، هزینه‌های مربوط به تجهیزات رایانه‌ای است. (نماین و شیرزاد، ۱۳۹۹)

➤ تهدیدهای الکترومغناطیس

تهدیدهای الکترومغناطیسی با استفاده از پالس الکتریکی ارسالی می‌تواند کلیه وسایل الکتریکی و الکترونیکی را از بین ببرد. فرودگاهی را تصور کنید که در خاموشی مطلق قرار گرفته است و هیچ خدماتی برای مسافران نمی‌تواند اجرا کند. اگر تهدید متوجه دستگاه‌های کمک ناوبری شود و هواپیما موفق به ناوبری هوایی خود نشود و یا نتواند فرود موفق داشته باشد، خطر بزرگی این صنعت رو تهدید می‌کند. پالس‌های الکترومغناطیس را به‌صورت ثابت و یا متحرک با استفاده از هواپیما و یا پمپا در هر نقطه‌ای می‌توان بکار برد و امنیت هوانوردی را به خطر انداخت (شیخی‌وند و همکاران، ۱۳۹۵).

➤ تهدیدهای زیست‌محیطی، شیمیایی، هسته‌ای

تروریسم زیست‌محیطی به معنای انتشار عمدی ویروس‌ها، باکتری‌ها، یا سایر میکروب‌ها بوده که درصدد ایجاد بیماری یا مرگ‌ومیر در میان انسان‌ها، جانوران، یا گیاهان، مورد استعمال قرار می‌گیرد. از مسائل عمده و برجسته قرارداد پکن، جرم‌انگاری بارگیری و تخلیه سلاح‌های بیولوژیکی، شیمیایی و هسته‌ای (مانند اورانیوم غنی‌سازی شده، مواد منفجره هسته‌ای و مواد رادیواکتیو) است؛ چراکه

1. (FAA) Federal Aviation Administration

2. (NASA) The National Aeronautics and Space Administration

گسترش استفاده از انرژی هسته‌ای و حساسیت مواد هسته‌ای همچون غنی‌سازی، فعالیت‌های باز فرآوری و سایر مواد حساس هسته‌ای شرایطی را ایجاد خواهند کرد که امکان استفاده از هواپیمای مسافربری را برای حمل و نقل چنین موادی فراهم می‌آورد (شناسایی، ۱۳۹۹). شکل ۲ چالش‌های امنیت فرودگاه‌ها را نشان می‌دهد.



شکل ۲ چالش‌های امنیت فرودگاه‌ها

فناوری

فناوری مجموع فنون، مهارت‌ها، روش‌ها و فرایندهایی است که در تولید کالاها یا خدمات یا تحقق اهداف مانند تحقیقات علمی استفاده می‌شود. فناوری می‌تواند دانش فن‌ها، فرایندها و مواردی از این دست باشد یا می‌تواند در ماشین‌ها تعبیه شود تا بدون اطلاع دقیق از عملکرد آن‌ها، امکان کار را فراهم آورد (Wikipedia).

فناوری نوین باعث ارتقاء، پیشرفت و نوآوری در حوزه فناوری‌های قبلی شده و راهکارهای جدیدی را در مسیر استفاده از فناوری‌ها پیش روی ما قرار می‌دهد. ویژگی‌های فناوری‌های نوین تعاملی بودن، فردی شدن، کنترل از سوی مخاطبان، تکثر و فراوانی، نفوذ، تحرک، تمرکززدایی، جهان‌گرایی، تبدیل‌پذیری، اتصال‌پذیری و توان مشارکت بسیار بالا است.

تعدادی از مطالعات بر روی راه‌حل استفاده از فناوری‌های استفاده از شناسایی پیشرفته زیست‌سنج

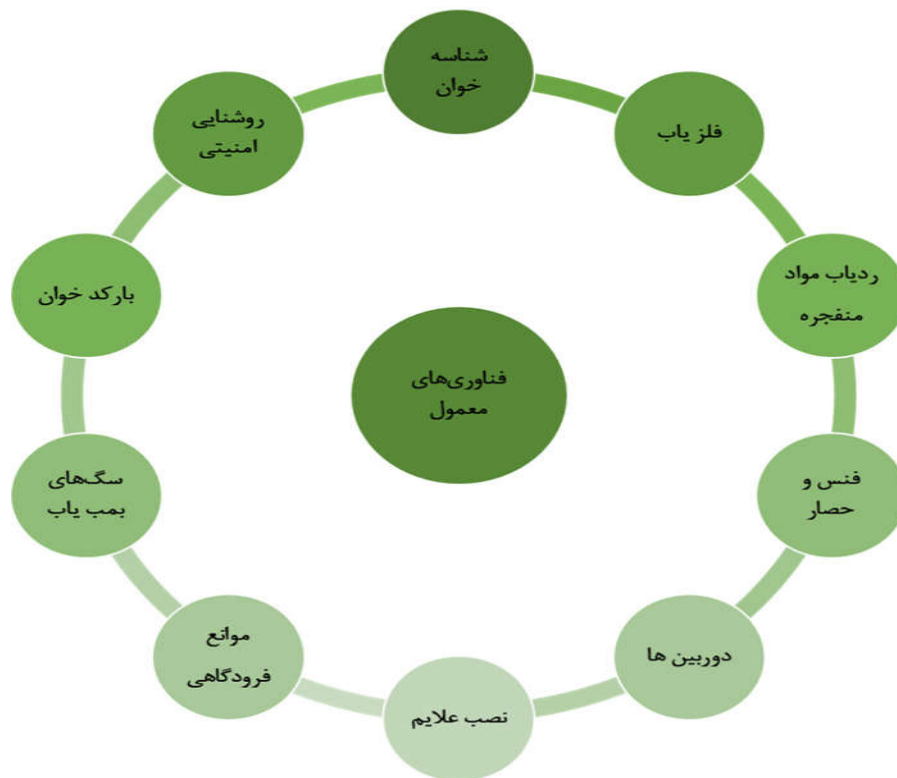
و فناوری‌های تجسم مبتنی بر هوش مصنوعی انجام شده است. معرفی چنین فن‌هایی به کاهش منابع و افزایش توان عملیاتی کاهش روش‌های غربالگری مسافران کمک می‌کند و همچنین باعث شناسایی سریع مسافران مستعد خطرناک و تهدیدات احتمالی می‌شود.

دسته‌بندی فناوری‌ها برای بهبود امنیت فرودگاه

- دسته اول فناوری‌های معمول، مانند فلزیاب برای جست‌وجوی مسافر و اسکن بار با استفاده از اشعه ایکس که در اکثر فرودگاه‌های جهان مورداستفاده قرار می‌گیرند.
- دسته دوم فناوری‌های نوین، مانند فناوری تشخیص چهره، هوش مصنوعی که در تعدادی از فرودگاه‌ها برحسب اهمیت و حساسیت بکار گرفته شده‌اند و در حال گسترش به سایر فرودگاه‌ها نیز هستند.
- دسته سوم فناوری‌های نسل بعدی (آینده) مانند فناوری زیست‌سنج رفتاری و دروازه امنیتی هوشمند که برخی از فرودگاه‌های جهان در حال تحقیق و آزمایش در این خصوص هستند (Zhang, 2019).

➤ فناوری‌های معمول امنیت فرودگاه‌ها

- فناوری‌های معمول اکثر فرودگاه‌های جهان از آن استفاده می‌کنند و در دو مرحله زیر انجام می‌گیرد.
- در مرحله اول اسناد هویتی و مدارک مسافرتی به همراه کارت پرواز مسافر، توسط افسر امنیت (با اسکن دوبعدی) بررسی می‌شود و بررسی می‌گردد. در صورت مطابقت داشتن مدارک و اعتبار کارت پرواز در مرحله بعد
 - در مرحله دوم غربالگری مسافران و بار همراه در سه مرحله انجام می‌شود.
- مرحله اول: از مسافر خواسته می‌شود چمدان و کلیه وسایل که با خود حمل می‌کند را روی تسمه ماشین اشعه ایکس قرار دهد و لپ‌تاپ و وسایل الکترونیکی باید از مسافر جدا شده و به صورت مجزا بررسی گردند. مسافر باید کفش کمربند و ژاکت خود را در بیاورد و جیب‌هایش رو خالی کند.
- مرحله دوم: از مسافر خواسته می‌شود که از میان فلزیاب حرکت کند. در صورت همراه داشتن فلز هشدار دستگاه به صدا درمی‌آید.
- مرحله سوم: اگر مسافر نیاز به غربالگری ثانویه داشته باشد افسر امنیتی مسافر را از ردیاب فلزی به سمت غربالگری ثانویه به صورت دستی و بازرسی بدنی هدایت می‌کند ممکن است وسایل در حضور مسافر، بر روی میز بازرسی شود و یا توسط یک ردیاب مواد منفجره به صورت تصادفی بازرسی صورت گیرد. شکل ۳ فناوری‌های معمول امنیتی فرودگاه‌ها را نشان می‌دهد.



شکل ۳ فناوری‌های معمول امنیت فرودگاه‌ها

فناوری‌های نوین

میزان سفرهای هوایی در قرن بیست و یک به شدت رشد کرده است و در نتیجه می‌توان فرودگاه‌ها را یکی از ارکان رشد حمل‌ونقل کالا و مسافر برای هر کشوری در نظر گرفت. فرودگاه‌ها در سال‌های اخیر بسیار پیشرفته‌تر شده‌اند. امروزه خدماتی که مسافران دریافت می‌کنند، گسترده شده است. در نتیجه پیچیدگی و تغییر در نوع رفتارهای مداخله غیرقانونی که کاربرهای فرودگاه با آن مواجه هستند نیز بیشتر گردیده است. کارکنان حفاظت اکنون با خطرهای مانند حمله‌های تروریستی، سرقت و تهدیدهای داخلی روبه‌رو هستند.

از نظر اکثر محققین سامانه امنیت فرودگاه، می‌توان به یک موضوع کلی اشاره کرد که سامانه امنیت فرودگاه‌ها با معرفی فناوری‌ها و روش‌های جدید بهبود می‌یابد. از طرفی روش‌های اجرای اقدامات تروریستی و سایر تهدیدها نیز از نظر فناوری پیشرفت کرده است.

امروزه بحث رفتارهای مداخله غیرقانونی هوانوردی و جرائم سازمان‌یافته و لزوم توجه به آن‌ها وارد مرحله جدیدی شده است. به‌نحوی که سعی می‌شود به طریق گوناگون، پیشگیری مؤثری از شکل‌گیری این جرائم به عمل آید. با پیشرفت روزافزون دستاوردهای بزرگی در زمینه افزایش امنیت صنعت هوانوردی برداشته شده است. پیشرفت در فناوری‌های نوین به دلیل نیاز جامعه و جهان است که باعث کاهش تخلفات، افزایش امنیت، تسریع در امور روزمره شده است. مرتکبین این گونه رفتارهای مداخله غیرقانونی همواره از پیشرفته‌ترین و به‌روزترین فناوری‌ها بهره می‌گیرند؛ بنابراین، به‌تناسب پیشرفت سریع فناوری، نیاز به روش‌های مطمئن تأیید هویت افراد هم بیشتر احساس می‌شود. شکل ۴ شمای کلی شناسایی فناوری‌های نوین برای ارتقای امنیت فرودگاه‌ها را نشان می‌دهد.



شکل ۴ شناسایی فناوری‌های نوین برای به‌کارگیری در ارتقای امنیت فرودگاه‌ها

➤ فناوری زیست‌سنج^۱ (تشخیص الگو)

بیومتریک یا زیست‌سنج، از یک کلمه یونانی «بیو» به معنای زندگی و «متریک» به معنای اندازه‌گیری تشکیل شده است. امروزه در زمینه‌های فراوانی ما به وسایلی نیاز داریم که هویت اشخاص را شناسایی و بر اساس ویژگی‌های بدن اشخاص آن‌ها را بازشناسی کند. فناوری زیست‌سنج عبارت است از روش‌های خودکار بررسی صحت یا شناسایی هویت شخص زنده (انسان‌ها) بر اساس مشخصات فیزیولوژیکی یا رفتاری (هاتف، ۱۳۸۶).

1. Biometrics

زیست‌سنج از مهم‌ترین و دقیق‌ترین سامانه‌های تشخیص هویت است. کاربرد این فناوری در استفاده از خصوصیات کاملاً منحصر به فرد فیزیولوژیکی و رفتاری افراد است. ثبت، تجزیه و تحلیل و سپس پردازش پارامترهای فوق، روشی است که باعث افزایش امنیت، دقت، سرعت و تسهیل در تعیین هویت اصلی و واقعی، شناسایی دقیق افراد و همچنین کاهش تخلف‌ها و مانع تقلب افراد سودجو و کنترل دسترسی‌های غیرمجاز می‌گردد. یک سامانه زیست‌سنجی، اساساً یک سامانه تشخیص الگوست که هویت اشخاص را با استفاده از اطلاعات زیست‌سنجی آن‌ها، تعیین یا تأیید می‌نماید. اولین قدم در راه استفاده از این سامانه‌ها ثبت اطلاعات زیست‌سنجی فرد در بانک داده سامانه است (بنده‌بی و عندلیب، ۱۳۹۵). گذرنامه زیست‌سنجی ترکیبی از صفحه‌های کاغذ و اسناد شناسایی الکترونیکی افراد است که از مشخصات زیست‌سنجی برای تصدیق شهروندی افراد استفاده می‌شود. اطلاعات کلیدی گذرنامه روی یک ریزتراشه رایانه‌ای بسیار کوچک ذخیره می‌گردد که بسیار شبیه به ذخیره اطلاعات بر روی کارت‌های هوشمند است. این گذرنامه‌ها اطلاعات شخص را بر روی ریزتراشه بدون تماس که به صورت نهفته در گذرنامه قرار دارد ثبت می‌نمایند. این ریزتراشه قادر است اطلاعات امضای دیجیتال را برای اطمینان از صحت گذرنامه و اطلاعات زیست‌سنجی در خود نگاه دارد (هاتف، ۱۳۸۶).

➤ فناوری تشخیص چهره

فناوری تشخیص چهره در واقع نوعی شناسایی دیجیتالی افراد است. این فناوری که مبتنی بر دانش هوش مصنوعی و یادگیری ماشین است، گامی فراتر از روش‌هایی مانند اسکن عنبیه و اثر انگشت یا شناسایی الگوهای رگ کف دست است که در حال حاضر برای تشخیص و تأیید هویت استفاده می‌شوند. سامانه‌های تشخیص چهره با استفاده از الگوریتم‌های رایانه‌ای جزئیات خاص و مشخصی را در چهره فرد انتخاب می‌کنند. این جزئیات، مانند فاصله بین چشم یا شکل چانه، عرض بینی، فرورفتگی گوشه لب‌ها یا بینی است. این اندازه‌ها سپس به فرمول‌های ریاضی تبدیل می‌شوند و با داده‌هایی که از چهره‌های دیگر جمع‌آوری شده، در یک پایگاه داده تشخیص چهره مقایسه می‌شوند. داده‌های مربوط به یک چهره خاص اغلب «الگوی چهره» نامیده می‌شوند و از یک عکس متمایز است؛ زیرا فقط برای جزئیات خاصی طراحی شده است که می‌تواند برای احراز هویت استفاده شود.

➤ فناوری اینترنت اشیا^۱

اینترنت اشیا (IoT) به اتصال دستگاه‌های هوشمند برای جمع‌آوری داده‌ها اشاره دارد (Panarello) و همکاران، (۲۰۱۸). سامانه‌ای از دستگاه‌های محاسباتی، ماشین‌های مکانیکی و دیجیتال، اشیا، حیوانات یا افراد است که با شناساگرهای یکتایی مشخص شده‌اند و توانایی انتقال داده در شبکه را بدون نیاز به تعاملات انسان با انسان یا انسان با رایانه دارند. با استفاده از حسگرهای مناسب (متصل به پلتفرم

1. (IoT) Internet of Things

اینترنت اشیا) حرکت افراد و وسایل نقلیه را در بخش‌های مختلف فرودگاه می‌توان با دقت کنترل کرد. در این حالت، سامانه‌عامل‌های اینترنت اشیا نه تنها امکان نظارت و جمع‌آوری داده‌های به‌دست‌آمده را فراهم می‌کنند، بلکه می‌توانند آن را تجزیه و تحلیل کرده و متخصصان را از تهدیدهای احتمالی آگاه سازند تا بتوانند خیلی سریع‌تر واکنش نشان دهند.

➤ فناوری شناسایی از طریق فرکانس رادیویی (RFID)¹

فناوری RFID تأثیر بسزایی در ارائه کارآمد حمل و نقل و توزیع و هدایت چمدان در صنعت هوانوردی داشته است. این فناوری قطعات الکترونیکی فرستنده و گیرنده را به صورت یک سامانه یکپارچه تبدیل می‌کند فرستنده‌ها معمولاً با نام تگ (برچسب) شناخته می‌شوند که با اتصال به چمدان می‌تواند باعث شناسایی بسته شوند (رستگار و هوشمند، ۱۳۹۷). از این فناوری در قسمت‌های مسیریابی، بلیت، بار مسافر، محموله‌ها و جلوگیری از جعل اسناد و مدارک در فرودگاه‌ها استفاده می‌شود (Sedláčková, 2021).

از برچسب‌های RFID به سفارش مالک‌ها در قسمت‌های مختلف هواپیما می‌تواند در بحث نظارتی و امنیتی استفاده شود. در بحث مسافر و بار همراه در مرحله پذیرش مجهز به دو برچسب RFID با اطلاعات یکسان مسافر، یک برچسب به کارت پرواز و برچسب دوم به بار همراه مسافر متصل می‌شود. در تمامی مسیرهای مورد نظر همچنین درب انبارها و کابین هواپیما مجهز به حس‌گرهایی به منظور شناسایی مسافر و بار همراه در نظر گرفته شده است؛ بنابراین، در هر نقطه می‌توان وضعیت مسافر و بار همراه او را در تحت نظارت داشت و در صورت سوار نشدن مسافر و یا وجود چمدان سرگردان، اقدام لازم انجام گردد (رادمنش و همکاران، ۱۳۹۶).

اطمینان از اینکه اگر چمدانی داخل هواپیما بارگیری شده است، مسافر مربوط به آن چمدان نیز سوار هواپیما شده است یا خیر مهم است. شرایطی را در نظر بگیرید که شخصی بمبی را در چمدان خود جاسازی کرده و پس از اینکه چمدان خود را برای بارگیری در هواپیما تحویل پذیرش می‌دهد، خود شخص متواری شده و سوار هواپیما نمی‌شود. این گونه موارد می‌بایست شناسایی شده و بسته‌های مذکور قبل از پرواز از هواپیما تخلیه گردند. این مورد به لحاظ امنیتی بسیار حائز اهمیت بوده و برای جلوگیری از انجام فعالیت‌های تروریستی ضروری است. گم شدن چمدان‌ها در فرودگاه و یا رها کردن چمدان‌های که مشکل امنیتی دارند یکی از مشکلات بزرگ در حین سفر است؛ اما با استفاده برچسب‌های تشخیص‌دهنده هوشمند با فرکانس رادیویی (RFID) و اپلیکیشن‌های ردیابی چمدان‌ها این مشکل مدیریت می‌گردد (رستگار و هوشمند، ۱۳۹۷).

1. Radio Frequency Identification

➤ فناوری هوش مصنوعی^۱

هوش مصنوعی به هوشی گفته می‌شود که یک ماشین در شرایط مختلف از خود نشان می‌دهد. به عبارت دیگر، هوش مصنوعی به سامانه‌های گفته می‌شود که می‌توانند واکنش‌هایی مشابه رفتارهای هوشمند انسانی، از جمله شرایط پیچیده، شبیه‌سازی فرایندهای تفکری، شیوه‌های استدلالی انسانی و پاسخ موفق به آن‌ها، یادگیری و توانایی کسب دانش و استدلال برای حل مسائل را داشته باشد. در سال ۲۰۱۷ هوش مصنوعی به معنای واقعی وارد صنعت حمل‌ونقل هوایی شد. تشخیص چهره یکی دیگر از کاربردهای هوش مصنوعی در مناطق دارای نظارت امنیتی بالا در جهان است.

➤ فناوری مسیرهای امنیتی هوشمند

استفاده از این مسیرها که باعث صرفه‌جویی در زمان و کاهش استرس مسافران می‌شود، به سرعت در سراسر جهان در حال گسترش است. بهره‌گیری از این مسیرها موجب افزایش سرعت انتقال بار مسافران به هواپیما و همچنین افزایش سرعت بازرسی و یافتن اشیای ممنوعه می‌شود. با این فناوری مسافران بدون آن‌که کمر بند یا لباس‌های خود را درآورند، از دروازه‌های امنیتی عبور می‌کنند. در فرودگاه دبی یک آکواریوم تونل‌مانند ساخته شده است که مسافران برای بازدید از ماهی‌ها از داخل این تونل عبور می‌کنند. با حرکت سر مسافرها، دوربین‌های امنیتی صورت و بدن آن‌ها را از همه زوایا شناسایی می‌کنند. با این کار، مأموران می‌توانستند، به راحتی، هویت افراد را تشخیص دهند.

➤ فناوری رباتیک^۲

رباتیک، شاخه‌ای میان‌رشته‌ای از مهندسی و علم است که شامل مهندسی مکانیک، مهندسی برق، علوم رایانه و چند رشته دیگر می‌شود. این فناوری دربردارنده فرایندهای طراحی، ساخت، راه‌اندازی و استفاده از ربات‌ها است، مواردی مانند سامانه‌های رایانه‌ای، کنترل، بازخورد حسگرها و پردازش اطلاعات نیز در این گروه قرار می‌گیرند. بسیاری از ربات‌ها در زمینه انجام شغل‌های خطرناک، مانند خنثی‌سازی بمب فعالیت می‌کنند که از این فناوری می‌توان در کمک به نیروهای امنیتی در فرودگاه‌ها و هواپیماها استفاده کرد. در زمینه بحث ربات‌های کنترل فرودگاه نباید از ربات‌های نگهبان و گشت‌زنی در فرودگاه چین بگذریم. این ربات‌ها Anbot نام دارند و به شکل بیضی هستند. همه این ربات‌ها دارای یک صفحه نمایش دیجیتال و یک دوربین با کیفیت بالا برای گرفتن عکس از مسافران و تجزیه و تحلیل آن‌ها دارند. نقش این دستگاه‌ها در حال حاضر، شبیه به یک دوربین امنیتی و به معنای واقعی ربات‌های کنترل فرودگاه هستند. آن‌ها همچنین به یک سازکار دفاعی که یک بازوی الکتریکی است و جریان الکتریکی تولید می‌کند، مجهز شده‌اند.

1. Artificial intelligence
2. Robotics

➤ بلاک چین^۱

بلاک چین به زنجیره‌ای از بلاک‌ها گفته می‌شود که اطلاعات را در بردارند (اعلم شاهی، ۱۳۹۶). اصلی‌ترین هدف در استفاده از فناوری مانند بلاک چین امکان به اشتراک‌گذاری داده‌ها به روشی ایمن و غیرقابل دست‌کاری برای شرکت‌های فرودگاه است، برای محقق‌شدن این هدف بلاک چین داده‌ها را با استفاده از قوانین پیچیده ریاضی و نرم‌افزاری ذخیره می‌کند و بنابراین هکرها و مهاجمان کار راحتی برای دست‌کاری و یا هک داده‌ها نخواهند داشت و از همه مهم‌تر حفظ امنیت دستگاه‌های متصل به اینترنت اشیا را به عهده دارد. اینترنت اشیا با اتصال دستگاه‌های هوشمند برای جمع‌آوری داده‌ها و تصمیم‌گیری هوشمند استفاده می‌شود. عدم وجود اقدامات امنیتی ذاتی، اینترنت اشیا را در معرض تهدیدهای حریص خصوصی و امنیتی قرار می‌دهد و برای حفظ امنیت سایبری نیاز به فناوری بلاک چین داریم.

علیرغم توسعه سریع محاسبات ابری، امنیت داده‌ها و محاسبات قابل‌اعتماد همچنان چالش‌های اصلی در برنامه‌های فعلی رایانش ابری وجود دارد. به‌منظور حل این مشکل، بسیاری از محققان تحقیقات زیادی در این مورد انجام داده‌اند و مدل‌های زیادی از جمله آزمون یکپارچگی داده‌ها و محاسبه امن چندجانبه را پیشنهاد کرده‌اند. با این حال، اکثر این راه‌حل‌ها با مشکلاتی مانند پیچیدگی محاسباتی بیش‌ازحد یا عدم مقیاس‌پذیری مواجه هستند. استفاده از فن‌های بلاک چین در سازکار امنیتی رایانش ابری برای بهبود عملکرد ذخیره‌سازی امن و محاسبات امن، است. (Wei و همکاران، 2020)

➤ واقعیت مجازی^۲ و واقعیت افزوده^۳

فناوری‌ای که با عنوان «واقعیت مجازی» شناخته شده است، محیطی را برای کاربر شبیه‌سازی می‌کند که در دنیای واقعی وجود ندارد. درواقع، کاربر با کمک یک هدست یا یک سخت‌افزار می‌تواند خود را در محیطی ببیند که در واقعیت وجود ندارد، ولی کاملاً حس واقعی را به او القاء می‌کند. این محیط‌ها اغلب به‌صورت سه‌بعدی یا ۳۶۰ درجه هستند. در حال حاضر، شبیه‌سازی واقعیت مجازی برای آموزش بهتر در انواع مختلف هواپیماها به کمک خلبانان آمده است. خلبانان می‌توانند از طریق مجازی و سناریوهای واقعی مختلف، به انواع گوناگون کابین خلبان دسترسی پیدا کرده و شرایط مختلف آب و هوایی را برای آزمون میزان استرس، بدون خطر و هزینه سنگین، شبیه‌سازی کنند. این گونه محیط‌های شبیه‌سازی شده می‌توان برای آشنایی کارکنان امنیتی فرودگاه به سناریوهای مختلف طرح‌های اضطراری فرودگاه در مقابل تهدیدات فرودگاه استفاده شود.

در فرودگاه چنانگی سنگاپور فناوری واقعیت افزوده در قالب عینک هوشمند دستورالعمل‌های مربوط به کارکنان را اجرایی می‌کند. به‌عنوان مثال، اسکن محموله بار هواپیما با عینک‌های هوشمند واقعیت افزوده

1. Blockchain

2. Virtual Reality

3. Augmented Reality

وقتی یک محموله بار روی زمین قرار دارد، این عینک هوشمند می‌تواند بارکد مجازی برای آن تعریف کند و آن را اسکن کرده و محتویات آن را رصد کند. با این عینک به‌صورت سریع می‌توان محتویات بار یا محموله را رصد و چک کرد. دوربین‌های نصب‌شده در عینک هوشمند نیز اجازه می‌دهد تا کارکنان مرکز کنترل بتوانند نظارت دقیقی بر محموله بار داشته باشند. این عینک هوشمند می‌تواند در زمان واقعی اطلاعات را به اتاق کنترل منتقل کند و کارکنان اتاق کنترل هم در جریان همه‌چیز قرار می‌گیرند.

➤ فناوری استفاده از پرنده‌های بدون سرنشین

قابلیت‌ها و کاربردهای این فناوری با سرعت زیادی در حال افزایش است. در برنامه‌های امنیتی فرودگاه می‌توانند برای گشت‌زنی، نظارت بر «سامانه‌های تشخیص نفوذ محیطی»^۱ و واکنش به زنگ هشدار سامانه‌ها، ردیابی تهدید، بازرسی بصری مناطق دورافتاده فرودگاه و بسیاری موارد دیگر استفاده شود. فرودگاه‌هایی بین‌المللی مانند ساوانا هیلتون و دالاس یا فورت ورث، استفاده از پرنده‌های بدون سرنشین به‌عنوان بخشی از برنامه‌های عملیاتی معمول خود برای بازرسی استفاده می‌کنند. به کارگیری «هواپیماهای بدون سرنشین» در عملیات فرودگاه برای برنامه‌های امنیتی فرودگاه، مانند ارزیابی فرودگاه، کنترل، بازرسی هواپیماها و زیرساخت فرودگاه بکار گرفته می‌شود. امنیت محیطی فرودگاه طیف گسترده‌ای از چالش‌ها را به همراه دارد. علاوه بر مناطق بزرگ‌تر نقاط ورودی جزئی متعددی مانند انبارها سوخت و سایر مکان‌های آسیب‌پذیر وجود دارد که باید محافظت شوند.

(Ashirbek, 2022)

➤ سامانه اطلاعات جغرافیایی (GIS)^۲

چهره کلیدی در سامانه امنیتی فرودگاه رئیس امنیت فرودگاه است که مسئول نظارت و سازمان‌دهی رویدادهای امنیتی فرودگاه است. اجرای کلیه وظایف محول‌شده، تصمیمات مناسب مدیریتی، اجرای موفق آن‌ها و دستیابی به اهداف تعیین‌شده توسط سازمان، به میزان شایستگی و سرعت تصمیم‌های گرفته شده بستگی دارد (Koryakina و همکاران، ۲۰۲۱). چنین تصمیماتی بر اساس داده‌های دریافتی از کاربرها و کارکنان از طریق کانال‌های ارتباطی داخلی است که باعث تأخیر زمانی در مراحل پاسخ می‌شود. کارآمدترین دریافت داده‌ها زمانی امکان‌پذیر است که داده‌ها مستقیماً از منبع (حسگر) به یک واحد منتقل شود و سامانه‌ای وجود داشته باشند که در آن داده‌ها از تمام دستگاه‌های سامانه امنیتی نمایش داده شود.

که شامل موارد زیر است

- سامانه امنیتی یکپارچه
- سامانه‌های اطلاعات جغرافیایی

1. (PIDS) Perimeter Intrusion Detection systems
2. Geographic information system

سامانه اطلاعات جغرافیایی (GIS) امکان ترکیب با سامانه امنیتی یکپارچه را فراهم می‌سازد. مزایای اصلی این روش اتصال از مختصات مکانی و زمانی در صورت بروز هرگونه حادثه و انتقال تصویر کامل از آنچه در حال رخ دادن است. موارد در زمان واقعی ضبط شده و به یک نقشه واحد منتقل می‌شود که به‌طور قابل توجهی زمان پاسخگویی تهدید و زمان خنثی سازی را کاهش می‌دهد.

عملیات GIS در پیکربندی‌های مختلف است؛ اما اصلی‌ترین آن‌ها یک برنامه نقشه کشی رایانه رومیزی است، بر اساس آن فرایندهای امنیتی از یک اتاق کنترل نظارت می‌شوند و یک برنامه شبکه که به رئیس سرویس امنیتی اجازه می‌دهد تا وضعیت یک شیء را در هر زمان از یک دستگاه تلفن همراه ردیابی کند و تصمیم مدیریتی درست را بگیرد در نتیجه زمان پاسخ و خنثی سازی تهدید را به‌طور قابل توجهی افزایش می‌یابد. GIS مدیریت مؤثر امنیت را با استفاده از آگاهی موقعیتی از قلمرو فرودگاه و امکانات موجود در فرودگاه ممکن می‌سازد؛ افزون بر این، به‌طور دقیق مختصات اشیاء، مناطق و قلمروها را نشان می‌دهد و اجازه تجزیه و تحلیل جامع از اشیاء کنترل شده را می‌دهد. در آینده، امکان گسترش استفاده از GIS از سرویس امنیتی به کل مجموعه فرودگاه وجود دارد که باعث بهبود شاخص‌های عملکردی فرودگاه می‌شود. کاهش زمان کلیه فعالیت‌های بازرسی، ثبت نام و همچنین سطح خدمات‌رسانی به مسافران را بهبود می‌بخشد.

➤ فناوری پیشرفته اشعه ایکس^۱

تمام وسایل شخصی که وارد هواپیما می‌شوند توسط فناوری پیشرفته اشعه ایکس نظارت و بررسی می‌شوند. سامانه‌های فناوری پیشرفته اشعه ایکس، مجهز به چندین منبع اشعه ایکس ثابت هستند که در توانش یکسانی، در حال حاضر، حدود ۱۴۰ کیلوولت تنظیم شده‌اند. تشعشع‌های الکترومغناطیسی یا فوتون‌های منابع پرتو ایکس به داخل دستگاه نفوذ می‌کنند و به اجسام می‌تابد سپس برنامه‌های شناسایی و تشخیص، می‌توانند اشیاء تهدید خاص را بر اساس یک کتابخانه آموزش دیده، مشخص کنند.

➤ فناوری تصویربرداری پیشرفته (AIT)^۲

ماشین‌های فناوری تصویربرداری پیشرفته، از تشعشع‌های الکترومغناطیسی غیر یونیزان، برای تشخیص اشیاء پنهان شده روی بدن مسافر بدون تماس فیزیکی استفاده می‌کنند. هنگامی که مسافر وارد دستگاه می‌شود و ثابت می‌ایستد، فرستنده‌ها امواج میلی متری تولید می‌کند که در حین عبور از لباس از روی پوست فرد جذب، پراکنده یا منعکس شده و سپس هرگونه توانش جهش تهدید به گیرنده‌ها برمی‌گردد. فناوری تصویربرداری پیشرفته الگوریتم‌های لازم را با سیگنال‌های «امواج میلی متری» (MMW)^۳ منعکس شده روی بدن برای تعیین محل ناهنجاری‌های احتمالی اعمال می‌کند. اگر یک ناهنجاری را

1. Advanced Technology X-ray
2. Advanced Imaging Technology
3. Millimeter Wave

تشخیص دهد، یک کادر محدودکننده آن مکان روی تصویر عمومی انسان نشان می‌دهد. یک کاربر باید وارد عمل شود و زنگ هشدار را با ضربه زدن قطع کند. کل زمان پردازش برای این سامانه، از شروع اسکن تا تصمیم‌گیری خودکار، کمتر از شش ثانیه است.

در آینده، فناوری تصویربرداری پیشرفته یک جزء کلیدی برای نظارت و بازرسی مسافران خواهد بود و الگوریتم‌های قابل تطبیق با انعطاف‌پذیری بیشتر برای افزایش امنیت بدون تعویض کل دستگاه در اختیار ما قرار می‌دهد. نسل بعدی فناوری تصویربرداری پیشرفته، وضوح تصویر بهبودیافته و با استفاده از آنتن‌های با باند وسیع برای کمک به «تشخیص پیشرفته تهدید به صورت خودکار» الگوریتم‌های تشخیص ارائه خواهد کرد؛ افزون بر این، بر روی الگوریتم‌های بازسازی سه‌بعدی برای شناسایی تهدیدهای پنهان در مکان‌های مبهم بدن تمرکز خواهد کرد.

➤ سامانه تشخیص مواد منفجره (EDS)^۱

سامانه تشخیص مواد منفجره از فناوری محاسبه توموگرافی (CT) computed tomography برای بازرسی چمدان‌های تحویل‌شده در باجه برای بارگیری در هواپیما استفاده می‌کند. داخل دستگاه سامانه تشخیص مواد منفجره، «سی تی» به صورت چرخشی، اسکن اجسام توسط اشعه ایکس را انجام می‌دهد. از این داده‌ها می‌توان برای اندازه‌گیری خواص فیزیکی (چگالی، عدد اتمی) محتویات چمدان و مقایسه آن با مواد تهدیدکننده انفجاری شناخته‌شده، استفاده کرد.

➤ مسیر امنیتی هوشمند^۲

فن‌های بینایی رایانه‌ای کنونی در هنگام تجزیه و تحلیل تصاویر محدود است. با این حال، پیشرفت‌های اخیر در شبکه‌های عصبی (چهارچوبی از الگوریتم‌های یادگیری ماشین که با قدرت هوش مصنوعی) و ظرفیت بالای تراشه‌های رایانه‌ای به دستگاه‌های هوش مصنوعی اجازه شکوفایی داده است که از نظارت هوشمند در حین عبور مسافر که از هوش مصنوعی استفاده شده است. در این روش مسافر نیاز به درآوردن کت و یا سایر اقلام از جیب خود نیست و یادگیری ماشین اجازه شناسایی تهدید از غیر تهدید را در کمتر از چند ثانیه هنگام عبور از اسکنر بدون توقف به وجود می‌آورد. در این روش دیگر نیازی به اسکن مجزا برای لب تاپ و مایعات و سایر اقلام نیست و مسافر می‌تواند با چمدان خود وسایل را از پست‌های بازرسی امنیتی حمل کند.

➤ دروازه امنیتی هوشمند^۳

در این فناوری ترکیبی از دوربین، تشخیص چهره و فناوری‌های موج میلی‌متری برای افراد که در حال عبور از یک دروازه امنیتی هستند استفاده می‌شود. فن‌های یادگیری ماشین از تجزیه و تحلیل خودکار داده‌ها برای

1. Explosives Detection System
2. Artificial intelligence Walk-through Scanner
3. Artificial intelligence Security Gate

شناسایی تهدید از غیر تهدید استفاده می‌کنند و در عرض یک ساعت حدود ۹۰۰ نفر از دروازه امنیتی می‌توانند عبور کنند و این بسیار سریع‌تر از پویشرهای معمولی است. (Zhang, 2019)

➤ فناوری زیست‌سنج رفتاری^۱

انتظار می‌رود، انگشت‌نگاری، تشخیص چهره و اسکن شبکه، به‌طور فزاینده‌ای برای اهداف امنیتی بکار رود. محققان دانشگاه منچستر انگلستان اخیراً یک سامانه هوش مصنوعی راه‌گسترش داده‌اند که الگوی راه رفتن افراد را به هنگام راه رفتن اندازه‌گیری می‌کند. درجایی دیگر با بودجه اتحادیه اروپا یک برنامه هوش مصنوعی برای تسریع امنیت و کنترل مرزها آزمایش شده است که شامل کارکنان مجازی است که از مسافران سؤال می‌پرسد، (مثلاً در چمدان شما چیست؟) درحالی که حالات چهره او توسط دوربین تجزیه و تحلیل می‌شود. اگر مسافر دروغ بگوید اطلاعات زیست‌سنج بیشتری از او گرفته می‌شود و برای تجدیدنظر به یک افسر انسانی منتقل می‌شود. نکته اصلی در استفاده از این فناوری دقت است. آزمایش‌های اولیه صورت گرفته موفقیت این طرح ۷۶ درصد است. با آموزش و به‌کارگیری برنامه‌های هوشمندتر نرخ موفقیت این طرح به ۸۵ درصد رسیده است.

تفکیک‌کننده‌های اضافی

افسرهای امنیتی هنگامی که یک مسافر یا چمدان او را بررسی می‌کند، به دنبال اقلام ممنوعه، مواد منفجره دست‌ساز و مواد منفجره خانگی هستند که می‌توانند خواص بسیار متغیری داشته باشند. برخلاف اکثر مواد منفجره تجاری و مواد منفجره نظامی که با کنترل دقیق بررسی می‌شوند. برای بررسی مؤثرتر این مواد منفجره، اداره امنیت حمل‌ونقل آمریکا (TSA)^۲ درحال توسعه قابلیت‌های اضافی است که تفکیک‌کننده بین اشیای بی‌خطر و تهدیدهای احتمالی و تشخیص مواد منفجره دست‌ساز خواهد بود. TSA همچنین با شرکای خود درحال توسعه الگوریتم‌های پیشرفته‌ای که می‌تواند ماشین‌های AT و CT را ارتقا دهند، مانند مغایرت فاز تشخیص، پراش اشعه ایکس و یادگیری عمیق هستند. (Karoly, 2017)

➤ مغایرت فاز تشخیص (DPC)^۳

مغایرت فاز تشخیص امکان تعیین عمق بیشتری از خواص مواد را در داخل یک فضای سه‌بعدی فراهم می‌کند و اطلاعات اضافی را برای تمایز بین تهدیدها و اشیای بی‌خطر به غربال‌گر ارائه می‌کند. درنتیجه هشدارهای کاذب را کاهش داده و فرایند نظارت را کارآمدتر می‌کند. هدف مشارکت با دانشگاه و صنعت هدف توسعه اجزای یک سامانه قابل اعتماد و مقرون‌به‌صرفه (سخت‌افزاری و نرم‌افزاری) که امکان پویشرهای (اسکن) پیشرفته چمدان با مغایرت مرحله تشخیص را فراهم می‌کند.

1. Behavioral Biometric Technology

2. Transportation Security Administration

3. Differential Phase Contrast

➤ پراش اشعه ایکس (XRD)^۱

پراش اشعه ایکس (XRD) به ماهیت دوگانه موج یا ذره اشعه ایکس برای به‌دست‌آوردن اطلاعات برای مطالعه ساختار مواد کریستالی استفاده می‌شود. ناحیه پرتو X در طیف الکترومغناطیس در محدوده بین پرتو و فرابنفش قرار دارد. با استفاده از این ناحیه طیفی می‌توان اطلاعاتی در خصوص ساختار، جنس ماده و نیز تعیین مقادیر عناصر به دست آورد. از این‌رو روش‌های پراش پرتو X در شیمی تجزیه کاربرد زیادی دارند. برای یک ماده خالص، الگوی پراش پرتو X، همانند اثرانگشت برای آن ماده است. تاکنون الگوی پراش بیش از ۷۵۰۰۰ ترکیب معدنی و آلی جمع‌آوری شده است. با استفاده از این پایگاه داده و با کمک روش جست‌وجو و تطبیق می‌توان ترکیب هر ماده را مشخص نمود. توموگرافی XRD مواد تهدیدکننده را که بسیار خواص مشابه به مواد بی‌خطر دارند، متمایز می‌کند، کاهش نرخ هشدار کاذب و ایجاد تمایز اضافی، برای تعیین اینکه آیا یک ماده حاوی ترکیبات انفجاری است یا خیر، استفاده می‌شود و می‌توانیم توان عملیاتی در پست‌های بازرسی فرودگاه افزایش دهیم.

➤ یادگیری عمیق^۲

یادگیری عمیق راهی برای غربال‌گری خودکار موارد ممنوعه از جمله مواد منفجره، اسلحه گرم و اشیاء تیز ارائه می‌کند. یادگیری عمیق (ماشینی) از الگوریتم‌های پیشرفته‌ای استفاده می‌کند که شکل شناسایی را با حجم مواد مقایسه می‌کند؛ مانند عدد اتمی ماده و اندازه‌گیری چگالی، سپس آن را با یک کتابخانه اقلام اسکن‌شده بسیار بزرگ مقایسه می‌کند. این کار به یک نتیجه «بد» یا «خوب» می‌انجامد. یک نتیجه «بد» نشان می‌دهد که ممکن است یک کالای ممنوعه در کیف فرد وجود داشته باشد. با گسترش کتابخانه، الگوریتم قادر به یادگیری و ما را به سمت شناسایی کاملاً خودکار سلاح‌ها، مواد منفجره و اقلام ممنوعه سوق می‌دهد.

توسعه رایانه‌ای توانش مشکلات محرمانه‌بودن، اخلاقیات و امنیت سایبری را دارد. امکان جاسوسی از اطلاعات وجود دارد، برخی معتقدند با افزایش سریع زیست‌سنج و فناوری تصویربرداری حفظ حریم خصوصی کم‌رنگ می‌شود. در پاسخ به نگرانی حفظ حریم خصوصی مربوط به نرم‌افزار «تشخیص هدف خودکار» پوششگرها (اسکنرها) یک تصویر کلی از یک شخص چه زن و چه مرد به‌صورت یکسان ارائه می‌کنند و اگر مورد مشکوکی تشخیص داده شد به‌صورت یک طرح کلی در نمایشگر نشان داده می‌شود و جزئیات بدن نمایش داده نمی‌شود. از نظر پوششگرها در «فناوری عبور از دروازه هوشمند» و «مسیر هوشمند» تصاویر به دلیل تشریحی بودن، هیچ مشکل اخلاقی ارائه نمی‌کند. ولی اگر سامانه هوش مصنوعی فرودگاه غیرفعال شود عواقب فاجعه‌باری به همراه دارد؛ بنابراین، جدیدترین و قدرتمندترین سامانه امنیت سایبری برای جلوگیری از هک دستگاه‌ها باید به کار گرفته شود.

1. X-ray Diffraction
2. Deep Learning

روش گردآوری داده‌ها

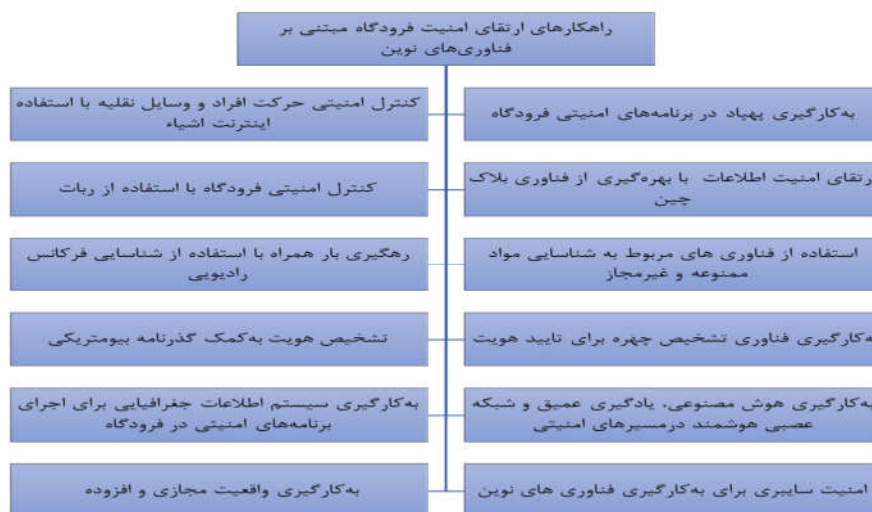
در تحقیق حاضر از دو شیوه کتابخانه‌ای و میدانی برای گردآوری اطلاعات استفاده شده است. برای گردآوری اطلاعات در این پژوهش ابتدا، از روش کتابخانه‌ای و اسنادی استفاده شده است؛ پس‌از آن، به بررسی و مطالعه قوانین و استانداردهای بین‌المللی، بر اساس اسناد و ضمایم سازمان هواپیمایی کشوری درباره امنیت فرودگاه‌ها پرداخته شده است؛ در ادامه برای بررسی و کسب اطلاعات هر چه بیشتر، برای شناخت دقیق‌تر موضوع موردپژوهش و استفاده از یافته‌های تحقیقات انجام‌شده در این زمینه، به بررسی و مطالعه پژوهش‌های پیشین داخلی و بین‌المللی پرداخته شده است.

جامعه آماری و نمونه

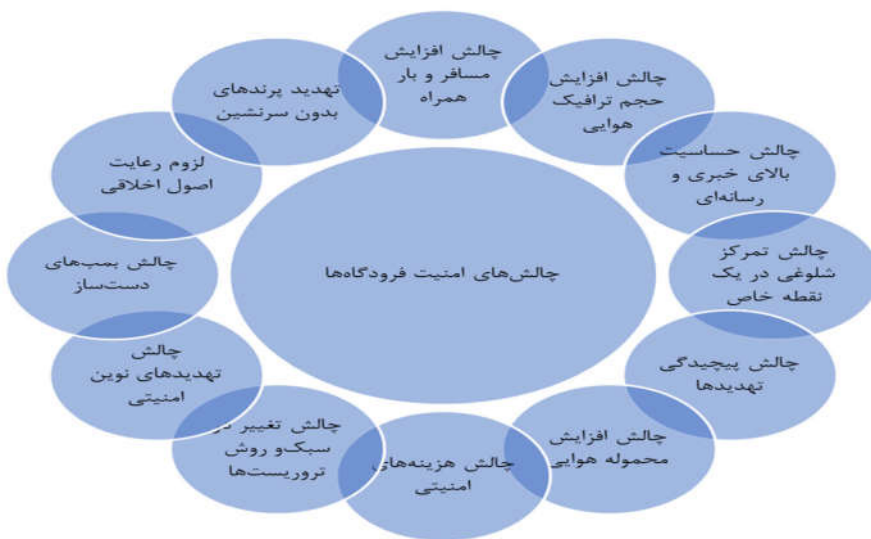
جامعه آماری این پژوهش شامل اساتید و نخبگان مرتبط با حوزه صنعت هوانوردی در دانشگاه هوایی شهید ستاری، دانشگاه صنعتی مالک اشتر، پایگاه‌های نیروی هوایی، مدیران ارشد و میانی فرودگاه‌ها، کارکنان امنیت پرواز، پلیس فرودگاه، حراست فرودگاه و مدیران شرکت‌های هواپیمایی در فرودگاه‌های بین‌المللی کشور هستند. از ۱۵۰ جایگاه کلیدی و نخبه شناسایی شده در این حوزه تعداد ۱۱۶ پرسش‌نامه تکمیل و جمع‌آوری شده و تحلیل‌های آماری بر این مبنا صورت گرفت.

روش گردآوری داده‌ها

راهکارهای اولیه از مبانی نظری و پیشینه پژوهش و سوابق به‌کارگیری فناوری‌ها در ارتقای امنیت فرودگاه‌ها و همچنین چالش‌های امنیت فرودگاه‌های کشورهای پیشرو حول محور ضمیمه ۱۷ سازمان بین‌المللی هوانوردی که درواقع مهم‌ترین سند در مورد امنیت هوانوردی است، جمع‌آوری شده است. سپس الگوی مفهومی اولیه راهکارها به‌صورت شکل‌های ۵ و ۶ تشکیل شدند.



شکل ۵ الگوی مفهومی اولیه راهکارهای ارتقای امنیت فرودگاه‌ها



شکل ۶ الگوی مفهومی چالش‌های امنیت فرودگاه‌ها

سپس، راهکارها و چالش‌های یادشده در اختیار تعداد ۵ نفر از خبرگان دانشگاهی و صنعت هوانوردی و همچنین اساتید راهنما و مشاور قرار گرفت و عوامل اولیه ضمن تعدیل به‌صورت جدول ۱ و ۲ استخراج

شد. پس از آن، پرسش‌نامه طراحی شد و مجدد برای بررسی در اختیار استادان و خیرگان صنعت هوانوردی قرار گرفت و پس از اخذ نظریات تکمیلی و تعدیل موادی از آن‌ها، در نهایت، پرسش‌نامه اصلی برای جمع‌آوری اطلاعات و نظرات خبرگان آشنا با امنیت فرودگاه‌ها و صنعت هوانوردی تنظیم و در اختیار جامعه آماری قرار گرفت.

در پرسش‌نامه این پژوهش از مقیاس ۵ درجه لیکرت که عبارت است از خیلی کم "۱"، کم "۲"، متوسط "۳"، زیاد "۴" و خیلی زیاد "۵" استفاده شده است و مقیاس پذیرفتنی برای پژوهش حاضر نتایج بزرگ‌تر از ۳ (زیاد و خیلی زیاد) است.

روش و ابزار تحلیل داده‌ها

در این پژوهش برای تحلیل داده‌ها از آمار توصیفی و استنباطی با کمک نرم‌افزارهای Excel و SPSS استفاده می‌شود. در بخش آمار توصیفی از شاخص‌های مرکزی و پراکندگی (میانگین و واریانس) و در آمار استنباطی با توجه به نرمال نبودن توزیع داده‌ها از آزمون دوجمله‌ای استفاده خواهد شد. همچنین آزمون فریدمن برای بررسی تفاوت اولویت راهکارهای شناسایی شده مورد استفاده قرار می‌گیرد.

روایی و پایایی پژوهش

گفتنی است که تأیید روایی پرسش‌نامه با استفاده از روایی محتوایی و صوری انجام شد. پایایی پرسش‌نامه نیز با استفاده از روش آلفای کرونباخ انجام شد و میزان آلفا برای تمامی سنج‌ها بالاتر از ۰/۸۷ به دست آمد و بنابراین پرسش‌نامه (ابزار تحقیق) دارای روایی و پایایی مناسب است.

جدول ۱ راهکارهای اولیه ارتقای امنیت فرودگاه‌ها مبتنی بر فناوری‌های نوین

ردیف	عنوان راهکار	فناوری‌های نوین استفاده شده
راهکار ۱	مسیرهای امنیتی هوشمند: (در این روش دیگر نیازی به اسکن مجزا برای لب تاپ و مایعات و سایر اقلام نیست و مسافران می‌توانند با چمدان خود از مسیرهای بازرسی عبور کنند)	هوش مصنوعی، یادگیری عمیق، شبکه‌های عصبی و بینایی کامپیوتری
راهکار ۲	دروازه (گیت) هوشمند: (تشخیص و شناسایی سریع هویت اشخاص)	هوش مصنوعی، یادگیری عمیق، تشخیص چهره و تصویربرداری پیشرفته
راهکار ۳	به کارگیری پرنده‌های بدون سرنشین در برنامه‌های امنیتی فرودگاه (نظارت و بازرسی بصری، تشخیص تهدید، اعلام هشدار، انتقال اطلاعات)	پرنده‌های بدون سرنشین
راهکار ۴	ارتقای امنیت اطلاعات با بهره‌گیری از فناوری بلاک چین	بلاک چین

ردیف	عنوان راهکار	فناوری‌های نوین استفاده شده
راهکار ۵	کنترل امنیتی فرودگاه با استفاده از ربات به جای کارکنان امنیتی	رباتیک
راهکار ۶	به کارگیری ربات برای انجام شغل‌های خطرناک در فرودگاه (مانند خنثی کردن بمب)	رباتیک
راهکار ۷	استفاده از فناوری تشخیص چهره برای تأیید هویت مسافر و کمک به گروه‌های حفاظتی فرودگاه در تشخیص، شناسایی و ردیابی مجرم‌ها	تشخیص چهره
راهکار ۸	تشخیص هویت به کمک گذرنامه زیست‌سنجی	زیست‌سنج
راهکار ۹	شناسایی امنیتی مسافران با استفاده از فناوری زیست‌سنج رفتاری (مانند الگوی راه رفتن) و تجزیه و تحلیل اطلاعات زیست‌سنجی	زیست‌سنج
راهکار ۱۰	شناسایی و ره‌گیری مسافر و بار همراه، با استفاده از فرکانس رادیویی	شناسایی فرکانس رادیویی
راهکار ۱۱	به کارگیری «سامانه اطلاعات جغرافیایی» برای شناسایی و واکنش سریع در مقابل تهدیدهای فرودگاه‌ها	سامانه اطلاعات جغرافیایی
راهکار ۱۲	نظارت و جلوگیری از ورود مواد منفجره با استفاده از «سامانه تشخیص مواد منفجره»	سامانه تشخیص مواد منفجره
راهکار ۱۳	تشخیص اشیاء پنهان شده روی بدن مسافر بدون تماس فیزیکی با به کارگیری فناوری «تصویربرداری پیشرفته»	تصویربرداری پیشرفته
راهکار ۱۴	به کارگیری «مغایرت فاز تشخیص» در پوششگرهای پیشرفته چمدان و تمایز بین اشیاء خطرناک و بی‌خطر با استفاده از خواص مواد	مغایرت فاز تشخیص
راهکار ۱۵	تشخیص ترکیبات انفجاری مواد با استفاده از «پراش اشعه ایکس»	پراش اشعه ایکس
راهکار ۱۶	نظارت و بازرسی محموله، بار با استفاده از عینک هوشمند	عینک هوشمند، واقعیت افزوده
راهکار ۱۷	شبیه‌سازی با فناوری واقعیت مجازی برای آموزش طرح‌های امنیتی فرودگاه	واقعیت مجازی

جدول ۲ چالش‌های امنیت فرودگاه‌ها

ردیف	عنوان
چالش ۱	افزایش حجم ترافیک هوایی
چالش ۲	افزایش مسافر و بار همراه
چالش ۳	تمرکز شلوغی در یک نقطه خاص
چالش ۴	حساسیت بالای مرکز خبری و رسانه‌ای فرودگاه
چالش ۵	افزایش محموله‌های هوایی

ردیف	عنوان
چالش ۶	پیچیدگی تهدیدها با توجه به رشد فناوری
چالش ۷	تغییر سبک و روش تروریست‌ها
چالش ۸	هزینه‌های زیاد امنیتی
چالش ۹	بمب‌های دست‌ساز
چالش ۱۰	لزوم رعایت اصول اخلاقی
چالش ۱۱	محرمانه‌بودن اطلاعات مسافران
چالش ۱۲	تهدید پرانده‌های بدون سر نشین
چالش ۱۳	تهدیدهای نوین

تجزیه و تحلیل داده‌ها

➤ سن جامعه آماری مورد مطالعه

جدول ۳ نشان‌دهنده سن جامعه آماری است. بر این مبنا می‌توان گفت بیش از نصف جامعه آماری این پژوهش در بازه سنی ۴۰ سال به بالا و حدود ۹۰ درصد بالای ۳۰ سال هستند.

جدول ۳ سن جامعه آماری

سن	فراوانی پاسخ	درصد فراوانی
زیر ۳۰ سال	۱۲	۱۰٫۳٪
۳۰-۴۰ سال	۴۴	۳۷٫۹٪
۴۱-۵۰ سال	۵۸	۵۰٪
۵۱ سال و بالاتر	۲	۱٫۷٪
جمع	۱۱۶	۱۰۰٪

➤ تحصیلات جامعه آماری مورد مطالعه

جدول ۴ نشان‌دهنده تحصیلات جامعه آماری است. بر این مبنا تقریباً ۵۶ درصد جامعه آماری دارای تحصیلات کارشناسی ارشد و بالاتر هستند.

جدول ۴ تحصیلات خبرگان مورد مطالعه

تحصیلات	فراوانی پاسخ	درصد فراوانی
کارشناسی	۶۰	۵۱٫۷٪
کارشناسی ارشد	۴۵	۳۸٫۷٪

تحصیلات	فراوانی پاسخ	درصد فراوانی
دکتری	۱۱	۹,۴٪
جمع	۱۱۶	۱۰۰٪

➤ سمت سازمانی جامعه آماری مورد مطالعه

جدول ۵ نشان‌دهنده سمت سازمانی جامعه آماری مرتبط با هوانوردی است. بر این مبنا تقریباً ۶۲ درصد از جامعه آماری این پژوهش در مشاغل مدیریتی و فرماندهی هوانوردی کشور هستند.

جدول ۵ سمت سازمانی جامعه آماری مرتبط با هوانوردی

سمت سازمانی	فراوانی پاسخ	درصد فراوانی
کارشناس	۴۵	۳۸,۸٪
معاون مدیریت	۱۷	۱۴,۷٪
مدیر میانی	۳۳	۲۸,۴٪
فرمانده	۲۱	۱۸,۱٪
مجموع	۱۱۶	۱۰۰٪

➤ سابقه جامعه آماری مورد مطالعه

جدول ۶ نشان‌دهنده سابقه جامعه آماری در ارتباط با صنعت هوانوردی است. بر این مبنا ۷۰ درصد جامعه آماری سابقه بالای ۱۵ سال در ارتباط با صنعت هوانوردی دارند، بر این اساس، افراد مورد مطالعه، دارای تجارب سازمانی بالایی هستند.

جدول ۶ سابقه مرتبط با هوانوردی جامعه آماری

سابقه	فراوانی پاسخ	درصد فراوانی
زیر ۱۰ سال	۱۵	۱۲,۹٪
۱۰-۱۵ سال	۲۰	۱۷,۲٪
۱۵-۲۰ سال	۲۴	۲۰,۶٪
۲۰-۲۵ سال	۴۰	۳۴,۴٪
بالای ۲۵ سال	۱۷	۱۴,۶٪
جمع	۱۱۶	۱۰۰٪

➤ آزمون نرمال بودن توزیع داده‌ها

به منظور بررسی نرمال بودن داده‌ها، از آزمون کولموگوروف – اسمیرنوف^۱ جدول ۷ استفاده شد. فرض صفر و فرض مقابل آماری برای این آزمون عبارت است از:

H_0 : توزیع داده‌های مربوط به الزامات امنیتی شناسایی شده نرمال است.

H_1 : توزیع داده‌های مربوط به الزامات امنیتی شناسایی شده نرمال نیست.

نتایج آزمون نشان داد که از آنجاکه سطح معناداری آزمون (sig) برای همه متغیرهای مورد بررسی کمتر از ۰/۰۵ به دست آمد، بنابراین فرض صفر آماری رد شده و ادعای نرمال بودن چالش‌ها و راهکارهای شناسایی شده تأیید نمی‌شود بر این مبنا از آزمون‌های ناپارامتریک برای تحلیل داده‌ها استفاده می‌شود.

جدول ۷ آزمون کولموگوروف – اسمیرنوف

عنوان	تعداد	میلگین	انحراف معیار	سطح معناداری
چالش ۱	۱۱۶	۳,۹۵	۹۹۲.	۰۰۰.
چالش ۲	۱۱۶	۳,۸۴	۷۹۸.	۰۰۰.
چالش ۳	۱۱۶	۴,۱۶	۶۵۹.	۰۰۰.
چالش ۴	۱۱۶	۴,۰۸	۷۸۲.	۰۰۰.
چالش ۵	۱۱۶	۳,۸۱	۸۱۲.	۰۰۰.
چالش ۶	۱۱۶	۴,۳۱	۷۸۵.	۰۰۰.
چالش ۷	۱۱۶	۴,۴۶	۷۰۳.	۰۰۰.
چالش ۸	۱۱۶	۳,۸۷	۸۶۰.	۰۰۰.
چالش ۹	۱۱۶	۳,۹۳	۸۶۲.	۰۰۰.
چالش ۱۰	۱۱۶	۳,۷۴	۸۵۶.	۰۰۰.
چالش ۱۱	۱۱۶	۳,۸۲	۹۷۴.	۰۰۰.
چالش ۱۲	۱۱۶	۴,۳۶	۷۶۲.	۰۰۰.
چالش ۱۳	۱۱۶	۴,۳۷	۸۷۰.	۰۰۰.
راهکار ۱	۱۱۶	۴,۵۲	۶۲۵.	۰۰۰.
راهکار ۲	۱۱۶	۴,۴۱	۶۷۲.	۰۰۰.
راهکار ۳	۱۱۶	۳,۹۵	۸۷۳.	۰۰۰.
راهکار ۴	۱۱۶	۱۱۴,	۷۷۸.	۰۰۰.
راهکار ۵	۱۱۶	۳,۸۹	۸۴۲.	۰۰۰.
راهکار ۶	۱۱۶	۴,۱۹	۹۰۳.	۰۰۰.

عنوان	تعداد	میلگین	انحراف معیار	سطح معناداری
راهکار ۷	۱۱۶	۴,۶۰	۵۷۳.	۰۰۰.
راهکار ۸	۱۱۶	۴,۴۵	۷۶۲.	۰۰۰.
راهکار ۹	۱۱۶	۴,۲۴	۸۰۹.	۰۰۰.
راهکار ۱۰	۱۱۶	۴,۲۳	۷۳۸.	۰۰۰.
راهکار ۱۱	۱۱۶	۴,۱۶	۷۸۷.	۰۰۰.
راهکار ۱۲	۱۱۶	۴,۳۹	۷۶۶.	۰۰۰.
راهکار ۱۳	۱۱۶	۴,۴۸	۶۷۹.	۰۰۰.
راهکار ۱۴	۱۱۶	۴,۳۸	۶۲۸.	۰۰۰.
راهکار ۱۵	۱۱۶	۴,۲۱	۸۰۳.	۰۰۰.
راهکار ۱۶	۱۱۶	۴,۰۳	۹۶۴.	۰۰۰.
راهکار ۱۷	۱۱۶	۴,۰۱	۸۹۹.	۰۰۰.

➤ بررسی تأیید راهکارها و چالش‌های شناسایی شده توسط خبرگان

به منظور بررسی پذیرش یا عدم پذیرش هر یک از چالش‌ها و راهکارهای امنیتی شناسایی شده برای ارتقای امنیت فرودگاه‌ها منطبق بر نظرات خبرگان، از آزمون دوجمله‌ای^۱ استفاده شده است، بدین منظور فرض صفر و فرض مقابل آماری به صورت زیر برای هر یک از متغیرها تعریف می‌شوند:

$$H_1: p > 0.5 \text{ و } H_0: p \leq 0.5$$

گفتنی است که p نسبت خبرگانی است که نظری مبنی بر تأثیر بیش از حد متوسط عوامل شناسایی شده بر روی موضوع مورد بررسی داشته‌اند.

از آنجایی که سطح معناداری آزمون (sig) برای تمام عوامل شناسایی شده به عنوان راهکارهای ارتقای امنیت فرودگاه‌ها و چالش‌های امنیت فرودگاه‌ها کمتر از سطح خطا (۰/۰۵) است؛ بنابراین نتایج با درصد قابل پذیرش انتخابی (۵۰ درصد) متفاوت است با مراجعه به درصد مشاهدات جدول ۸ متوجه خواهیم شد اکثر خبرگان راهکارها و چالش‌های شناسایی شده را بیش از حد متوسط (زیاد و خیلی زیاد) برای فرودگاه‌ها ضروری دانسته‌اند. در نتیجه برای کلیه موارد فرض صفر بالا رد شده و فرض مقابل آماری پذیرفته می‌شود؛ بنابراین راهکارهای شناسایی شده پذیرفته می‌شود.

جدول ۸ نتایج مرتبط با آزمون دو جمله‌ای

عنوان	گروه	طبقه	تعداد	درصد مشاهدات	درصد قابل پذیرش	سطح معناداری
چالش ۱	گروه ۱	$3 = >$	۳۱	۲۷.	۵۰.	۰۰۰.
	گروه ۲	$3 <$	۸۵	۷۳.		
	مجموع		۱۱۶	۱۰۰		
چالش ۲	گروه ۱	$3 = >$	۳۹	۳۴.	۵۰.	۰۰۰.
	گروه ۲	$3 <$	۷۷	۶۶.		
	مجموع		۱۱۶	۱۰۰		
چالش ۳	گروه ۱	$3 = >$	۱۷	۱۵.	۵۰.	۰۰۱.
	گروه ۲	$3 <$	۹۹	۸۵.		
	مجموع		۱۱۶	۱۰۰		
چالش ۴	گروه ۱	$3 = >$	۲۹	۲۵.	۵۰.	۰۰۰.
	گروه ۲	$3 <$	۸۷	۷۵.		
	مجموع		۱۱۶	۱۰۰		
چالش ۵	گروه ۱	$3 = >$	۴۲	۳۶.	۵۰.	۰۰۴.
	گروه ۲	$3 <$	۷۴	۶۴.		
	مجموع		۱۱۶	۱۰۰		
چالش ۶	گروه ۱	$3 = >$	۱۷	۱۵.	۵۰.	۰۰۰.
	گروه ۲	$3 <$	۹۹	۸۵.		
	مجموع		۱۱۶	۱۰۰		
چالش ۷	گروه ۱	$3 = >$	۱۲	۱۰.	۵۰.	۰۰۰.
	گروه ۲	$3 <$	۱۰۴	۹۰.		
	مجموع		۱۱۶	۱۰۰		
چالش ۸	گروه ۱	$3 = >$	۳۹	۳۴.	۵۰.	۰۰۱.
	گروه ۲	$3 <$	۷۷	۶۶.		
	مجموع		۱۱۶	۱۰۰		
چالش ۹	گروه ۱	$3 = >$	۴۱	۳۵.	۵۰.	۰۰۲.
	گروه ۲	$3 <$	۷۵	۶۵.		
	مجموع		۱۱۶	۱۰۰		

عنوان	گروه	طبقه	تعداد	درصد مشاهدات	درصد قابل پذیرش	سطح معناداری
چالش ۱۰	گروه ۱	$3=>$	۴۳	۴۶.	۵۰.	۰۰۷.
	گروه ۲	$3<$	۷۳	۵۴.		
	مجموع		۱۱۶	۱۰۰		
چالش ۱۱	گروه ۱	$3=>$	۴۲	۳۶.	۵۰.	۰۰۴.
	گروه ۲	$3<$	۷۴	۶۴.		
	مجموع		۱۱۶	۱۰۰		
چالش ۱۲	گروه ۱	$3=>$	۱۳	۱۱.	۵۰.	۰۰۰.
	گروه ۲	$3<$	۱۰۳	۸۹.		
	مجموع		۱۱۶	۱۰۰		
چالش ۱۳	گروه ۱	$3=>$	۲۲	۱۹.	۵۰.	۰۰۰.
	گروه ۲	$3<$	۹۴	۸۱.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱	گروه ۱	$3=>$	۸	۰۷.	۵۰.	۰۰۰.
	گروه ۲	$3<$	۱۰۸	۹۳.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۲	گروه ۱	$3=>$	۱۰	۰۹.	۵۰.	۰۰۰.
	گروه ۲	$3<$	۱۰۶	۹۱.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۳	گروه ۱	$3=>$	۳۹	۳۴.	۵۰.	۰۰۱.
	گروه ۲	$3<$	۷۷	۶۶.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۴	گروه ۱	$3=>$	۲۷	۲۳.	۵۰.	۰۰۰.
	گروه ۲	$3<$	۸۹	۷۷.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۵	گروه ۱	$3=>$	۳۸	۳۳.	۵۰.	۰۰۰.
	گروه ۲	$3<$	۷۸	۶۷.		
	مجموع		۱۱۶	۱۰۰		

عنوان	گروه	طبقه	تعداد	درصد مشاهدات	درصد قابل پذیرش	سطح معناداری
راهکار ۶	گروه ۱	$3 >$	۱۹	۱۶.	۵۰.	
	گروه ۲	$3 <$	۹۷	۸۴.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۷	گروه ۱	$3 >$	۵	۰۴.	۵۰.	
	گروه ۲	$3 <$	۱۱۱	۹۶.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۸	گروه ۱	$3 >$	۱۵	۱۳.	۵۰.	
	گروه ۲	$3 <$	۱۰۱	۸۷.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۹	گروه ۱	$3 >$	۲۴	۲۱.	۵۰.	
	گروه ۲	$3 <$	۹۲	۷۹.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۰	گروه ۱	$3 >$	۱۹	۱۶.	۵۰.	
	گروه ۲	$3 <$	۹۷	۸۴.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۱	گروه ۱	$3 >$	۲۴	۲۱.	۵۰.	
	گروه ۲	$3 <$	۹۲	۷۹.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۲	گروه ۱	$3 >$	۱۲	۱۰.	۵۰.	
	گروه ۲	$3 <$	۱۰۴	۹۰.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۳	گروه ۱	$3 >$	۱۰	۰۹.	۵۰.	
	گروه ۲	$3 <$	۱۰۶	۹۱.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۴	گروه ۱	$3 >$	۹	۰۸.	۵۰.	
	گروه ۲	$3 <$	۱۰۷	۹۲.		
	مجموع		۱۱۶	۱۰۰		

عنوان	گروه	طبقه	تعداد	درصد مشاهدات	درصد قابل پذیرش	سطح معناداری
راهکار ۱۵	گروه ۱	$3 >$	۱۶	۱۴.	۵۰.	
	گروه ۲	$3 <$	۱۰۰	۸۶.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۶	گروه ۱	$3 >$	۳۷	۳۲.	۵۰.	
	گروه ۲	$3 <$	۷۹	۶۸.		
	مجموع		۱۱۶	۱۰۰		
راهکار ۱۷	گروه ۱	$3 >$	۳۱	۲۷.	۵۰.	
	گروه ۲	$3 <$	۸۵	۷۳.		
	مجموع		۱۱۶	۱۰۰		

➤ اولویت‌بندی راهکارهای ارتقای امنیت فرودگاه‌ها و چالش‌های مربوطه

به منظور بررسی اولویت‌بندی (رتبه‌بندی)، راهکارهای ارتقای امنیت فرودگاه‌ها و چالش‌های مربوطه از آزمون فریدمن^۱ استفاده شد، بدین منظور فرض صفر و فرض مقابل آماری به صورت زیر تعریف شدند:

H0: اولویت راهکارها و چالش‌های شناسایی شده مورد یکسان است.

H1: اولویت راهکارها و چالش‌های شناسایی شده متفاوت است.

از آنجاکه میزان سطح معناداری آزمون ۰/۰۰۰ به دست آمد و چون این میزان کمتر از سطح خطا (۰/۰۵)، است فرض صفر رد شد؛ بنابراین، راهکارها و چالش‌ها دارای اولویت متفاوتی هستند و بر مبنای خروجی آزمون فریدمن هر راهکار و چالشی که میانگین رتبه بالاتری داشته باشد اولویت بالاتری نسبت به سایرین از دیدگاه نخبگان دارد. جدول ۹ و ۱۰ همچنین شاخص‌های توصیفی مربوط به متغیرهای مورد مطالعه (میانگین، انحراف معیار، بیشینه و کمینه) ارائه شده، تأکید بر این نکته دارد که تمام راهکارها و چالش‌های شناسایی شده با میانگین بالایی مورد پذیرش نخبگان قرار گرفته‌اند. جدول ۱۱ و ۱۲

جدول ۹ نتایج آزمون فریدمن مربوط به راهکارهای ارتقای امنیت فرودگاه‌ها

عنوان	میانگین رتبه	اولویت
راهکار ۱	۱۰.۵۶	۲
راهکار ۲	۹.۹۶	۵
راهکار ۳	۷.۲۴	۱۶
راهکار ۴	۷.۹۴	۱۳

۱۷	۶,۷۶	راهکار ۵
۱۱	۸,۷۳	راهکار ۶
۱	۱۱,۱۴	راهکار ۷
۴	۱۰,۲۸	راهکار ۸
۸	۸,۸۴	راهکار ۹
۹	۸,۸۱	راهکار ۱۰
۱۲	۸,۳۶	راهکار ۱۱
۶	۹,۹۲	راهکار ۱۲
۳	۱۰,۴۵	راهکار ۱۳
۷	۹,۶۸	راهکار ۱۴
۱۰	۸,۸۰	راهکار ۱۵
۱۴	۷,۸۵	راهکار ۱۶
۱۵	۷,۶۲	راهکار ۱۷

آزمون فریدمن راهکارهای امنیت فرودگاه‌ها

۱۱۶	تعداد
۱۷۹,۷۴۱	مربع کای
۱۶	درجه آزادی
۰۰۰.	سطح معنی‌داری

جدول ۱۰ نتایج آزمون فریدمن مربوط به چالش‌های امنیت فرودگاه‌ها

عنوان	میانگین رتبه	اولویت
چالش ۱	۶,۷۶	۷
چالش ۲	۶,۰۹	۱۰
چالش ۳	۷,۳۵	۵
چالش ۴	۶,۹۰	۶
چالش ۵	۵,۶۹	۱۲
چالش ۶	۸,۲۴	۴

عنوان	میانگین رتبه	اولویت
چالش ۷	۸,۸۴	۱
چالش ۸	۶,۱۱	۹
چالش ۹	۶,۴۱	۸
چالش ۱۰	۵,۵۷	۱۳
چالش ۱۱	۶,۰۳	۱۱
چالش ۱۲	۸,۴۷	۳
چالش ۱۳	۸,۵۵	۲

آزمون فریدمن چالش‌های امنیت فرودگاه‌ها

۱۱۶	تعداد
۱۶۸,۸۹۵	مربع کای
۱۲	درجه آزادی
۰۰۰.	سطح معنی‌داری

جدول ۱۰ مقادیر آمار توصیفی برای راهکارهای ارتقای امنیت فرودگاه‌ها

ردیف	تعداد پاسخ	میانگین	انحراف معیار	بیشترین مقدار	کمترین مقدار	رتبه
راهکار ۱	۱۱۶	۴,۵۲	۶۳۵.	۵	۳	۲
راهکار ۲	۱۱۶	۴,۴۱	۶۷۲.	۵	۲	۵
راهکار ۳	۱۱۶	۳,۹۵	۸۷۳.	۵	۲	۱۶
راهکار ۴	۱۱۶	۴,۱۱	۷۷۸.	۵	۲	۱۳
راهکار ۵	۱۱۶	۳,۸۹	۸۴۲.	۵	۲	۱۷
راهکار ۶	۱۱۶	۴,۱۹	۹۰۳.	۵	۱	۱۱
راهکار ۷	۱۱۶	۴,۶۰	۵۷۳.	۵	۳	۱
راهکار ۸	۱۱۶	۴,۴۵	۷۶۲.	۵	۲	۴
راهکار ۹	۱۱۶	۴,۲۴	۸۰۹.	۵	۲	۸

ردیف	تعداد پاسخ	میانگین	انحراف معیار	بیشترین مقدار	کمترین مقدار	رتبه
راهکار ۱۰	۱۱۶	۴,۳۳	۷۳۸.	۵	۲	۹
راهکار ۱۱	۱۱۶	۴,۱۶	۷۸۷.	۵	۲	۱۲
راهکار ۱۲	۱۱۶	۴,۳۹	۷۶۶.	۵	۲	۶
راهکار ۱۳	۱۱۶	۴,۴۸	۶۷۹.	۵	۲	۳
راهکار ۱۴	۱۱۶	۴,۳۸	۶۲۸.	۵	۳	۷
راهکار ۱۵	۱۱۶	۴,۲۱	۸۰۳.	۵	۱	۱۰
راهکار ۱۶	۱۱۶	۴,۰۳	۹۶۴.	۵	۱	۱۴
راهکار ۱۷	۱۱۶	۴,۰۱	۸۹۹.	۵	۱	۱۵

جدول ۱۱ مقادیر آمار توصیفی برای چالش‌های امنیت فرودگاه‌ها

ردیف	تعداد پاسخ	میانگین	انحراف معیار	بیشترین مقدار	کمترین مقدار	رتبه
چالش ۱	۱۱۶	۳,۹۵	۹۹۲.	۵	۱	۷
چالش ۲	۱۱۶	۳,۸۴	۷۹۸.	۵	۲	۱۰
چالش ۳	۱۱۶	۴,۱۶	۶۵۹.	۵	۳	۵
چالش ۴	۱۱۶	۴,۰۸	۷۸۲.	۵	۲	۶
چالش ۵	۱۱۶	۳,۸۱	۸۱۲.	۵	۱	۱۲
چالش ۶	۱۱۶	۴,۳۱	۷۸۵.	۵	۲	۴
چالش ۷	۱۱۶	۴,۴۶	۷۰۳.	۵	۲	۱
چالش ۸	۱۱۶	۳,۸۷	۸۶۰.	۵	۲	۹
چالش ۹	۱۱۶	۳,۹۳	۸۶۲.	۵	۲	۸
چالش ۱۰	۱۱۶	۳,۷۴	۸۵۶.	۵	۱	۱۳
چالش ۱۱	۱۱۶	۳,۸۲	۹۷۴.	۵	۱	۱۱
چالش ۱۲	۱۱۶	۴,۳۶	۷۶۲.	۵	۱	۳
چالش ۱۳	۱۱۶	۴,۳۷	۸۷۰.	۵	۲	۲

جمع‌بندی و نتیجه‌گیری

با توجه به رفتارهای مداخله غیرقانونی گسترده و تهدیدهای نوین علیه امنیت فرودگاه‌ها، مطالعه راهکارها و تدابیر مختلف، برای ارتقای امنیت فرودگاه‌ها لازم و ضروری است. در این پژوهش که با هدف شناسایی و اولویت‌بندی راهکارهای ارتقای امنیت فرودگاه‌ها با تأکید بر فناوری‌های نوین انجام شده، پس از بررسی اسناد و ضمایم سازمان بین‌المللی هواپیمایی کشوری و همچنین مبانی نظری و پیشینه پژوهش‌های انجام شده در این حوزه در مجامع بین‌المللی و کشورهای پیشرو به طراحی مدلی مفهومی از راهکارهای ارتقای امنیت فرودگاه‌ها و در کنار آن چالش‌های امنیت فرودگاه‌ها پرداخته شده است. بعد از بررسی و تعدیل راهکارها و چالش‌ها توسط نخبگان دانشگاهی و صنعت هوانوردی، اقدام به جمع‌آوری نظرات نخبگان مربوطه و تجزیه و تحلیل داده‌ها شد و نتایج در دو قسمت راهکارها و چالش‌ها به دست آمد.

➤ **راهکارهای ارتقای امنیت فرودگاه‌ها مبتنی بر فناوری‌های نوین از دیدگاه نخبگان صنعت هوانوردی به ترتیب زیر اولویت‌بندی شدند:**

- ۱- استفاده از فناوری «تشخیص چهره» برای تأیید هویت مسافر و کمک به گروه‌های حفاظتی فرودگاه در تشخیص، شناسایی و ردیابی مجرم‌ها
- ۲- مسیرهای امنیتی هوشمند با استفاده از فناوری‌های هوش مصنوعی، یادگیری عمیق، بینایی رایانه‌ای و شبکه‌های عصبی
- ۳- تشخیص اشیاء پنهان شده روی بدن مسافر بدون تماس فیزیکی با به کارگیری فناوری «تصویربرداری پیشرفته»
- ۴- تشخیص هویت به کمک گذرنامه زیست‌سنجی
- ۵- دروازه (گیت) هوشمند با استفاده از فناوری‌های هوش مصنوعی، یادگیری عمیق و تشخیص چهره
- ۶- نظارت و جلوگیری از ورود مواد منفجره با استفاده از «سامانه تشخیص مواد منفجره»
- ۷- به کارگیری «مغایرت فاز تشخیص» در پوششگرهای پیشرفته چمدان و تمایز بین اشیاء خطرناک و بی‌خطر با استفاده از خواص مواد
- ۸- شناسایی امنیتی مسافران با استفاده از فناوری «زیست‌سنج رفتاری» (مانند الگوی راه رفتن) و تجزیه و تحلیل اطلاعات زیست‌سنجی
- ۹- شناسایی و ره‌گیری مسافر و بار همراه، با استفاده از فناوری «شناسایی فرکانس رادیویی»
- ۱۰- تشخیص ترکیبات انفجاری مواد با استفاده از «پراش اشعه ایکس»
- ۱۱- به کارگیری ربات برای انجام شغل‌های خطرناک در فرودگاه (مانند خشی کردن بمب)

۱۲- به کارگیری «سامانه اطلاعات جغرافیایی» برای شناسایی و واکنش سریع در مقابل تهدیدهای فرودگاه‌ها

۱۳- ارتقای امنیت اطلاعات با بهره‌گیری از فناوری «بلاک چین»

۱۴- نظارت و بازرسی محموله، بار با استفاده از «عینک هوشمند»

۱۵- شبیه‌سازی با فناوری «واقعیت مجازی» برای آموزش طرح‌های امنیتی فرودگاه

۱۶- به کارگیری «پرنده‌های بدون سرنشین» در برنامه‌های امنیتی فرودگاه (نظارت و بازرسی بصری، تشخیص تهدید، اعلام هشدار، انتقال اطلاعات)

۱۷- کنترل امنیتی فرودگاه با استفاده از «ربات» به جای کارکنان امنیتی فرودگاه‌ها

➤ **چالش‌های امنیت فرودگاه‌ها از دیدگاه نخبگان صنعت هوانوردی به ترتیب زیر اولویت‌بندی شدند:**

۱- تغییر سبک و روش تروریست‌ها

۲- تهدیدهای نوین

۳- تهدید پرنده‌های بدون سرنشین

۴- پیچیدگی تهدیدها با توجه به رشد فناوری

۵- تمرکز شلوغی در یک نقطه خاص

۶- حساسیت بالای مرکز خبری و رسانه‌ای فرودگاه

۷- افزایش حجم ترافیک هوایی

۸- بمب‌های دست‌ساز

۹- هزینه‌های زیاد امنیتی

۱۰- افزایش مسافر و بار همراه

۱۱- محرمانه‌بودن اطلاعات مسافران

۱۲- افزایش محموله‌های هوایی

۱۳- لزوم رعایت اصول اخلاقی

استفاده از فناوری‌های نوین برای ارتقای امنیت فرودگاه‌ها باعث کاهش خطای انسانی و افزایش سرعت نظارت و بازرسی می‌شوند؛ بنابراین مسافران در پشت دروازه‌های امنیتی که مکان‌های مستعد برای تهدیدهای تروریستی به شمار می‌آیند، معطل نمی‌شوند و همراه بارهای خود از مسیرهای هوشمند مشخص‌شده، بدون نیاز به گذرنامه و کارت پرواز تردد می‌کنند.

پیشنهادهای کاربردی

با توجه به مجموعه مطالعات انجام‌شده پیشنهاد می‌گردد:

- فرودگاه‌های کشور از راهکارهای ارائه‌شده برای ارتقای امنیت فرودگاه‌های کشور به ترتیب اولویت بیان‌شده در این پژوهش استفاده نمایند.
- مدیران حراست فرودگاه‌های کشور چالش‌های امنیتی فرودگاه‌ها را مطابق با اولویت ارائه‌شده مدنظر قرار داده و راهکارهای لازم را مبتنی بر فناوری‌های نوین بیان‌شده به کارگیرند.
- فرودگاه‌های دنیا در حال استفاده از فناوری‌های نوین در ابعاد امنیتی و خدماتی و گسترش آن‌ها هستند. به کارگیری فناوری‌های نوین فقط مختص به امنیت فرودگاه‌ها نیست و در هوشمند سازی فرودگاه‌ها نیز به کار گرفته می‌شوند؛ بنابراین، با توجه به موقعیت اقتصادی، فرهنگی و گردشگری کشور، حرکت به این سمت لازم و ضروری است.

منابع:

- اعلم شاهی، هادی (۱۳۹۶)، «مقدمه‌ای بر بلاک چین»، سومین کنفرانس ملی نوآوری و تحقیق در مهندسی برق و مهندسی رایانه و مکانیک.
- بنده پی، فرزانه؛ عندلیب، اعظم (۱۳۹۵)، «بررسی کاربرد زیست‌سنج در تشخیص هویت»، دومین کنفرانس بین‌المللی مدیریت و فناوری اطلاعات و ارتباطات، تهران.
- رادمنش، امین؛ محمدحسین، حمید؛ رادمنش، حمید (۱۳۹۶)، «ارتقای سامانه امنیت کاکبیت هواپیما با نصب سامانه نظارت ویدیویی در هواپیماهای ناوگان هوایی»، سومین کنفرانس ملی مهندسی مکانیک- عمران و فناوری‌های پیشرفته.
- رستگار، محمدعلی؛ هوشمند، هانیه (۱۳۹۷)، «کاربرد اینترنت اشیا در صنعت هوانوردی»، چهارمین کنفرانس ملی فناوری در مهندسی برق و کامپیوتر.
- شیخی‌وند، سبحان؛ حکاری، آرام؛ رموز نیکو (۱۳۹۵)، «بررسی بمب‌های الکترومغناطیسی بر سامانه‌های الکترونیکی و ارائه راهکارهای مقابله با آن»، کنفرانس پدافند غیرعامل و توسعه پایدار.
- شناسایی، هدایت‌الله (۱۳۹۹)، «تحلیل حقوقی تصویب کنوانسیون ۲۰۱۰ پکن در تقویت امنیت هوانوردی در پرتو رویکردهای بازدارندگی ایکائو»، پژوهش‌های حقوقی، شماره ۴۱.
- صابری، علیرضا (۱۴۰۱)، «شناسایی و اولویت‌بندی راهکارهای ارتقای امنیت فرودگاه‌ها با تأکید بر فناوری‌های نوین»، پایان‌نامه کارشناسی ارشد مهندسی عملیات هوانوردی، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران.
- نمایان، پیمان؛ شیرزاد، امید؛ (۱۳۹۹)، «جرم‌انگاری رفتارهای غیرقانونی علیه امنیت هوایمایی کشوری در قلمرو کنوانسیون ۲۰۱۰ پکن و پروتکل الحاقی آن»، فصلنامه علمی مطالعات بین‌المللی پلیس، دوره یازدهم، شماره ۴۱، صفحات ۲۰۹-۱۸۲، بهار.
- هاتف، مهدی (۱۳۸۶)، «زیست‌سنج رویکردی نوین در تأمین امنیت»، دوماهنامه توسعه انسانی پلیس، سال چهارم، شماره ۱۲، مرداد و شهریور.
- A. Ashirbek, "Analysis of the FAA's Small UAS Regulations for Airports Security Support UAS Operations", Arizona State University, 2022.
- <https://www.airbus.com/en/products-services/commercial-aircraft/market/global-market-forecast>, ed
- J. Bolton, "Airport Security Investment Model" University of Arkansas, 2017.
- V. Burlov, A. Andreev, and F. Gomazov, "Mathematical model of human decision-A methodological basis for the realization of the human factor in safety

- management**", *Procedia Computer Science*, vol. 145, pp. 112-117, 2018.
- <https://www.changiairport.com/corporate/media-centre/changijourneys/the-changi-experience/want-to-go-on-a-virtual-reality-tour-of-singapore.html>, ed.
 - http://www.china.org.cn/china/2016-09/22/content_39347636.
 - in <https://donyaye-hefazat.com/1399/articles/airport-security/>, ed.
 - D. Gillen and W. G. Morrison, "**Aviation security: Costing, pricing, finance and performance**", *Journal of Air Transport Management*, vol. 48, pp. 1-12, 2015.
 - ICAO; Annex 17, "**Security; Safeguarding International Civil Aviation Against Acts of Unlawful Interference**" Eleventh Edition, March 2020.
 - ICAO; Annex 14, volume I, "**aerodromes; aerodrome design and operations**" Eighth Edition, July 2018.
 - ICAO; Annex9, "**facilitation**" Fifteenth October 2017.
 - in <https://isiarticles.com/topic/469> ed.
 - B. A. Jackson and T. LaTourrette, "**Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries**", *Journal of Air Transport Management*, vol. 48, pp. 26-33, 2015.
 - N. Kagalwalla and P. P. Churi, "**Cybersecurity in aviation: An intrinsic review**", in 5th International Conference on Computing, Communication, Control and Automation (ICCUBE), IEEE, pp. 1-6, 2019.
 - S. Karoly, "**Technologies to counter aviation security threats**", in AIP Conference Proceedings, 2017, vol. 1898, no. 1: AIP Publishing LLC, p. 050002.
 - A. A. Kirschenbaum, "**The cost of airport security: The passenger dilemma**", *Journal of Air Transport Management*, vol. 30, pp. 39-45, 2013.
 - A. S. Koryakina, V. V. Gryzunov, and V. G. Burlov, "**Ways to Reduce the Time of Response to Threats to an Airport**", *IFAC-PapersOnLine*, vol. 54, no. 13, pp. 97-102, 2021.
 - University of Maryland Global Terrorism Database. (n.d.). Retrieved from Global Terrorism Database Website :<https://www.start.umd.edu/gtd/>
 - A. K. K. Orozobekova A.K., "**Geographic information systems and coordinate**

systems", Bulletin of KGUSTA, vol. 2, pp. 20-28, 2012.

- A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, **"Blockchain and iot integration: A systematic survey"**, Sensors, vol. 18, no. 8, p. 2575, 2018.
- <http://portalhamlonaghli.ir/fa/125131>
- J. Pyrgies, **"The UAVs threat to airport security: risk analysis and mitigation"**, Journal of Airline and Airport Management, vol. 9, no. 2, pp. 63-96, 2019.
- A. N. Sedláčková, **"Implementation of smart technologies into the civil aviation aircraft maintenance process"**, The Science and Development of Transport (ZIRP 2021), p. 123, 2021.
- J. Skorupski and P. Uchroński, **"Evaluation of the effectiveness of an airport passenger and baggage security screening system"**, Journal of Air Transport Management, vol. 66, pp. 53-64, 2018.
- D. Stevens, T. Schell, T. Hamilton, R. Mesic, and M. S. Brown, **"Near-term options for improving security at Los Angeles International Airport"**, RAND CORPARLINGTON VA, 2004
- M. G. Stewart and J. Mueller, **"Cost-benefit analysis of airport security: Are airports too safe?"**, Journal of Air Transport Management, vol. 35, pp. 19-28, 2014.
- M. G. Stewart and J. Mueller, **"Terrorism risks and cost-benefit analysis of aviation security"**, Risk Analysis, vol. 33, no. 5, pp. 893-908, 2013.
- P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, **"Blockchain data-based cloud data integrity protection mechanism"**, Future Generation Computer Systems, vol. 102, pp. 902-911, 2020.
- Z. Zhang, **"Technologies raise the effectiveness of airport security control"**, in 2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT), IEEE, pp. 431-434, 2019.