فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال سیزدهم: شمارهٔ ٤٦- بهار ١٤٠٣
صص: ١٣٩ - ١٦٩
تاریخ دریافت: ۱۴۰۳/۱۱/۲۸ تاریخ پذیرش: ۱۴۰۴/۰۴/۲۱

Quarterly of Passive Defense & Security
Vol.13, No.46,Spring 2024
P-P: 139 - 169

نقش هوش مصنوعی در فرایند مدیریت بحران‌های امنیتی

جمشید نصرت‌آبادی[۱]
پژمان غلام‌نژاد[۲]
حسین امیری[۳]

چکیده

هوش مصنوعی به یک عامل نوین قدرت تبدیل شده و رقابت‌های شدیدی بین کشورهای پیشرفته برای توسعه این فناوری در جریان است. در حال حاضر، هوش مصنوعی بیشتر در حوزه‌های پزشکی، کشاورزی، صنعت و اقتصاد کاربرد دارد و به‌زودی به سیاست نیز گسترش می‌یابد. با افزایش پیچیدگی و شدت بحران‌های امنیتی، استفاده از فناوری‌های نوین نظیر هوش مصنوعی جهت مدیریت بحران‌های امنیتی ضروری شده است. در همین راستا محقق در نظر دارد نقش هوش مصنوعی در فرایند مدیریت بحران‌های امنیتی موردبررسی نماید. در واقع این پژوهش در پی پاسخ به این سؤال است که هوش مصنوعی چگونه می‌تواند در فرایند مدیریت بحران‌های امنیتی و در ایجاد امنیت نقش ایفا نماید؟ که با استفاده از مطالعه اسناد و مدارک و نظرات صاحب‌نظران و ارائه سه فرضیه به‌عنوان عوامل مؤثر پیشنهادی محقق انجام شده است. جامعه آماری در این تحقیق با درنظرگرفتن یک ضریب خاص ۵۰ نفر و حجم نمونه نیز به‌صورت تمام شمار در نظر گرفته شده است. به‌منظور سنجش پایایی ابزار پرسش‌نامه از ضریب آلفای کرونباخ بر اساس هریک از متغیرها استفاده شده است که مقدار آلفای کرونباخ برای کل پرسش‌نامه معادل ۰/۸۴ محاسبه گردیده است. تحقیق انجام شده از نوع موردی - زمینه‌ای است و به‌منظور جمع‌آوری اطلاعات موردنیاز از روش جمع‌آوری میدانی (مصاحبه و پرسش‌نامه) و روش کتابخانه‌ای (مطالعه اسناد و مدارک) استفاده شده است. نتایج تحقیق بیانگر آن است که هوش مصنوعی در سه

۱. استادیار و عضو هیئت علمی دانشکده علوم و فنون فارابی (نویسنده مسئول) Dr.nosratabadi110@gmail.com
۲. کارشناس‌ارشد M.Hoseinpour@gmail.com
۳. دانشجوی کارشناسی‌ارشد S.Mohamadzade@gmail.com

مرحله قبل، حین، و بعد از بحران، قادر به جمع‌آوری و تجزیه‌وتحلیل داده‌ها، تشخیص تهدیدات و پیش‌بینی رویدادها، ارائه راهکارهای مناسب، بهبود زمان واکنش و تصمیم‌گیری و خودکارسازی فرایندها است. به‌طورکلی، این فناوری می‌تواند به شکل قابل‌توجهی کارایی و اثربخشی مدیریت بحران‌های امنیتی را افزایش دهد و به دولت‌ها و سازمان‌ها در حفظ امنیت جوامع کمک نماید.

واژه‌های کلیدی: امنیت، هوش‌مصنوعی، بحران امنیتی، جمع آوری اطلاعات، تصمیم‌گیری.

جستارگرایی

یک کشور به‌عنوان واحد سیاسی متشکل از سرزمین، جمعیت و حکومت با بحران‌های اقتصادی، فرهنگی، اجتماعی و سیاسی مواجه است (فیروزی، ۱۳۸۵: ۵۴). این بحران‌ها هرگاه با کنش‌های جمعی نظم مستقر را به چالش کشیده و اختلال در زندگی روزمره و ایجاد ناامنی کنند، ماهیت امنیتی می‌یابند (امیری، ۱۳۹۱:۲۲۰). افزایش آگاهی اجتماعی و ناکافی‌بودن پاسخ‌های دولتی زمینه‌ساز اعتراضات و شورش‌های خشونت‌آمیز می‌شود که تهدیدی برای امنیت ملی است؛ لذا مدیران باید با شناسایی دقیق آسیب‌ها و اتخاذ تدابیر مؤثر، از تشدید ناامنی جلوگیری کنند (رئیسی و همکاران، ۱۳۹۷:۷۶).

پرسش اصلی این پژوهش آن است که هوش‌مصنوعی[1] (AI) چگونه می‌تواند مدیران سازمان‌های اطلاعاتی و امنیتی را در مدیریت بحران‌ها یاری دهد. فرضیه‌ها نشان می‌دهد هوش‌مصنوعی در سه مرحله قبل، حین و پس از بحران با تحلیل سریع و دقیق داده‌ها، پیش‌بینی ریسک، تخصیص منابع، بهبود ارتباطات و کاهش هزینه و زمان، کارایی مدیریت بحران را افزایش می‌دهد(سان و همکاران،۲۰۲۰:۱). همچنین ادغام دوربین‌های مداربسته با برنامه‌های جستجوی تصویر و پایگاه‌های داده، امکان هشدار به‌موقع و رتبه‌بندی افراد مشکوک را فراهم می‌کند (رادولوف، ۲۰۱۹:۳).

این تحقیق با به‌کارگیری روش کتابخانه‌ای و میدانی (پرسش‌نامه و مصاحبه) و بررسی ۵۰ مدیر و کارشناس در حوزه‌های عملیاتی - امنیتی انجام شده است. ضریب آلفای

1. Artificial Intelligence

کرونباخ پرسش‌نامه برابر با ۰٫۸۴ محاسبه شد و داده‌ها از اسناد مکتوب، منابع اینترنتی و ابزارهای میدانی گردآوری گردید.

از منظر اهمیت و ضرورت؛ اهمیت این مطالعه ازآن‌جهت است که روش‌های سنتی توان مقابله با پیچیدگی و سرعت تحولات بحران‌ها را ندارند. هوش مصنوعی با تحلیل لحظه‌ای انبوه داده‌ها و ارائه راهکارهای هوشمند می‌تواند به‌عنوان ابزاری راهبردی در پیش‌بینی، پیشگیری و مدیریت بحران عمل کند؛ غفلت از این ظرفیت نه‌تنها هزینه‌ها را افزایش می‌دهد، بلکه ناامنی‌های گسترده‌تری به دنبال دارد.

مرتبط با پیشینه تحقیق، پژوهش‌های پیشین از جمله موضوعی با عنوان "کاربردهای هوش مصنوعی در مدیریت بحران‌ها" در مجله اسپرینجر[1] نشان می‌دهند که هوش مصنوعی با بهره‌گیری از الگوریتم‌های پیشرفته یادگیری ماشینی، شبکه‌های عصبی، الگوریتم‌های ژنتیکی و سیستم‌های چندعاملی، کارایی مدیریت بحران را به طور چشمگیری افزایش می‌دهد. بوچینی و داویسون (۲۰۲۰) در مطالعه‌ای جامع پیرامون بلایای طبیعی تأکید کردند که این فناوری می‌تواند سرعت پیش‌بینی خطر، مدیریت ریسک، حفظ محیط‌زیست و ارتباطات اضطراری را بهبود بخشد و هم‌زمان هزینه‌های کنترل بحران را کاهش دهد (بوچینی و همکاران،۲۰۲۰).

همچنین پژوهشی دیگر مبنی بر "کاربرد فناوری‌های هوش محاسباتی در مدیریت بحران" توسط لیوچن (۲۰۱۹) در مجله هوش مصنوعی[2] انجام گردیده، نشان داد که کاربرد هوش‌مصنوعی در مدیریت اضطراری، باعث تقویت کارآیی سیستم‌های واکنش سریع و آشکارسازی به‌موقع چالش‌های درمانده می‌شود. (لیوچن ، ۲۰۱۹)

در پژوهشی دیگر با موضوع "هوش مصنوعی و امنیت" که توسط رادولوف (۲۰۱۹) در مجله امنیت و آینده انجام گردیده در بررسی نقش هوش‌مصنوعی در امنیت سایبری و شبکه‌های اطلاعاتی، ثابت کرد که تشخیص الگوهای پیچیده تهدید و پیشگیری از نفوذ، مستقیماً متأثر از قدرت پردازش و تحلیل کلان‌داده‌های این فناوری است. (رادولوف،۲۰۱۹)

1. Springer
2. Artificial Intelligence

در پژوهشی دیگر با موضوع "هوش مصنوعی برای امنیت داخلی» که توسط وانگ (۲۰۰۵) در مجله سیستم‌های هوشمند انجام گردیده، نشان داد با تمرکز بر امنیت داخلی، امکان‌پذیری شناسایی و پیشگیری از تهدیدهای امنیتی را مؤثر دانست؛ هرچند محدودیت‌های قانونی و نیاز به هماهنگی میان‌بخشی را مانعی جدی برای کارآمدی کامل هوش مصنوعی برشمرد. (وانگ،۲۰۰۵)

در پژوهشی دیگر با موضوع « تحول نظریه و عمل مدیریت بحران امنیتی بین‌دولتی در چین» که توسط جانستون (۲۰۱۶) در مجله دانشگاه جنگ دریایی تحول نظریه و عمل مدیریت بحران امنیتی بین‌المللی در چین را بررسی کرد و به‌ویژه بر نقش تعاملات تاریخی و سیاسی در شکل‌دهی به استراتژی‌های هوشمند تأکید نمود.(جانستون،۲۰۱۶)

همچنین پژوهشی دیگر مبنی بر "امنیت منطقه‌ای در جنوب آسیا در پرتو هوش مصنوعی" توسط عباسیان (۱۴۰۰) در مؤسسه آینده‌پژوهی جهان اسلام دریافت که هوش مصنوعی عاملی دوپهلو است؛ از یک سو ضریب ایمنی زرادخانه‌های هسته‌ای و فضای سایبری را افزایش می‌دهد و از سوی دیگر، پیچیدگی معمای ثبات استراتژیک را تشدید می‌کند. (عباسیان،۱۴۰۰) درنهایت در پژوهشی دیگر مبنی بر "بررسی وضعیت فناوری هوش - مصنوعی در ایران و جهان" توسط عبدی (۱۳۹۶) در معاونت پژوهش‌های زیربنایی و امور تولیدی دفتر مطالعات ارتباطات و فناوری‌های نوین آینده به بررسی وضعیت فناوری هوش مصنوعی در ایران و جهان به مزایا و چالش‌های حقوقی و اخلاقی این سامانه‌ها اشاره کرد و هشدار داد که بدون سیاست‌گذاری و قانون‌گذاری مناسب، احتمال سوءاستفاده و ارتکاب جرم توسط یا با کمک هوش مصنوعی افزایش می‌یابد. (عبدی، ۱۳۹۶)

مفاهیم و مبانی نظری

ماهیت و ویژگی‌های بحران امنیتی

بحران امنیتی وضعیتی است که موجودیت یک کشور یا نظام حاکم و ارزش‌های اساسی آن را تهدید می‌کند. این بحران اغلب ماهیتی پیچیده و منحصربه‌فرد دارد و تدوین دستورالعملی کلی برای تمام رویدادها دشوار است. هر بحران امنیتی باید مطابق ویژگی‌های خاص خود مدیریت شود، زیرا هیچ جامعه‌ای به طور کامل از بروز

بحران مصون نیست. از این رو، وجود بحران به‌معنای بی‌ثباتی مطلق نبوده و ثبات مستلزم توانایی مدیریت مستمر این رویدادهاست (عارفی و همکاران، ۱۴۰۲ :۶۵).

اطلاعات و مدیریت اطلاعات در بحران

اطلاعات در مدیریت بحران، مجموعه‌ای از فعالیت‌ها و محصولات مرتبط با داده‌هاست که طی فرایندهایی مانند جمع‌آوری، تحلیل، ارزشیابی و تفسیر به شکل‌دهی به تصمیم‌گیری کمک می‌کند. هیلزمن سه فعالیت اصلی اطلاعات را شامل گردآوری داده‌ها، داوری و ارزیابی، و ارائه نتایج به سیاست‌گذاران می‌داند. وزارت دفاع آمریکا بر پردازش و تحلیل داده‌ها درباره نقاط مختلف جغرافیایی تأکید دارد و بارندز[1] نیز اطلاعات را محصول تحلیل تمام داده‌های مرتبط با فعالیت‌های خارجی می‌داند. گادسون[2] نقش دولت یا نهادهای خصوصی را در تولید و توزیع اطلاعات امنیتی برجسته می‌کند و رابرستون[3] معتقد است وجود تهدید، محرک اصلی فرایندهای اطلاعاتی است (محمودبابویی و همکاران، ۱۴۰۰: ۱۱).

در مدیریت بحران، دسترسی به اطلاعات مرتبط و به‌موقع کارکرد تصمیم‌گیری را تسهیل می‌کند. سه شاخص تصمیم در شرایط بحرانی عبارت‌اند از: مرحله اطمینان که اطلاعات کافی و دقیق در دسترس است، مرحله خطر که اطلاعات موجود ولی ناکافی است، و مرحله عدم اطمینان که کمبود اطلاعات تصمیم‌گیری را با مشکل مواجه می‌کند. سازمان‌های اطلاعاتی به‌عنوان مغز متفکر دستگاه‌های سیاسی و نظامی عمل کرده و با پیش‌بینی تهدیدات به پیشگیری و کنترل بحران کمک می‌کنند. مدل مدیریت اطلاعاتی بحران تلفیقی از فرایندهای کلان اطلاعاتی و اصول مدیریت برای پیش‌بینی، پیشگیری و مقابله است (حیدری، ۱۴۰۱: ۱۸-۱۹).

در فضای پرتنش سیاسی و مبهم که رنگ تهدید به خود گرفته، پدیدارشدن بحران‌های امنیتی آسان‌تر می‌شود. هرچه یک پدیده اجتماعی به سمت امنیتی‌شدن حرکت کند، دامنه گزینه‌های واکنش محدودتر و حساسیت نسبت به آن بیشتر می‌شود. . ماندل[4] تهدید امنیتی را فشاری داخلی یا خارجی می‌داند که توان کشور در دستیابی به اهداف

1. Brand's
2. Godson
3. Robertson
4. Robert Mundell

ملی را مختل کرده یا کیفیت زندگی مردم و اختیارات حکومت را به طورجدی کاهش می‌دهد. اگر واکنش به تهدید متناسب با شدت آن نباشد، کشور به بحران امنیتی کشیده خواهد شد (حبیبی و هادیان، ۱۳۹۵: ۲۲).

ویژگی‌های عمده بحران‌های امنیتی بر اساس آیین‌نامه پشتیبانی اطلاعاتی برای عملیات مشترک (۰- 2 JP) شامل موارد زیر است (همان: ۲۲):

- محدودیت زمانی بالا در عین گستردگی مکانی و شدت عمل
- هماهنگی و انطباق مؤثر بین سطوح تاکتیکی و راهبردی
- جریان سریع اطلاعات در لایه‌های مختلف
- تأثیر عمیق بر افکار عمومی
- اثرگذاری بر منافع ملی و اهداف سیاسی، راهبردی و حیاتی
- تشدید عملیات روانی و افزایش تأثیر اقدامات ویژه

مدیریت بحران امنیتی

در مدیریت بحران امنیتی، خود بحران هرچقدر هم که ماهیت متفاوتی داشته باشد، به‌طور همزمان موجب ایجاد تهدیدها و نیازمندی‌های امنیتی می‌شود. مدیریت بحران مجموعه‌ای از مفاهیم نظری و اقدامات عملی در سطوح سیاست‌گذاری، برنامه‌ریزی و سازماندهی است که با هدف مواجهه اثربخش و به‌موقع با وضعیت‌های بحرانی به‌کار می‌رود. معیار اصلی تمایز «بحران» از «مدیریت بحران»، روش‌های اتخاذی برای کنترل آن است؛ هرچه توانایی ایجاد موانع پیش‌گیرنده و کنترل بحران قوی‌تر باشد، موفقیت مدیریت نیز بالاتر خواهد بود (رئیسی و همکاران، ۱۳۹۸:۸۲).

الگوهای مدیریت بحران امنیتی

هیچ الگوی واحدی برای تمامی شرایط بحران امنیتی وجود ندارد و انتخاب بهترین چارچوب وابسته به ویژگی‌های محیطی، مأموریتی، ساختاری، ایدئولوژیک و راهبردی سازمان‌ها است. بااین‌حال، اغلب الگوها در سه محور کلی شناخت بحران، پیشگیری/ کنترل و بازسازی مشترک هستند؛ تفاوت‌های جزئی ناشی از ماهیت و سطح بحران است (ساوه درودی، ۱۴۰۰: ۸۳).

یکی از رایج‌ترین مدل‌ها، نظریه سه‌مرحله‌ای قبل، حین و بعد از بحران است که بر سه اولویت زیر متمرکز است(همان، ۱۴۰۰: ۸۵):

- پیشگیری (مرحله قبل از بحران)
- کاهش اثرات (مرحله حین بحران)
- ترمیم و بازسازی (مرحله بعد از بحران)

این مدل، اگرچه در ساده‌سازی فرایند کمک می‌کند، به پیش‌بینی دقیق بحران و ارائه راهبردهای جلوگیری از وقوع آن به‌اندازه کافی نپرداخته است.

پژوهشگران دیگری نظیر ریچاردسون[1] (۱۹۹۴) و لیچت[2] (۱۹۹۰) نیز همین سه مرحله را به‌عنوان زیربنای سیاست‌گذاری و برنامه‌ریزی مدیریت بحران مطرح کرده‌اند. آنها بر لزوم:

- پیش‌بینی و آمادگی سازمانی (مرحله قبل)
- اقدامات مقابله‌ای برای بازگرداندن نظم و امنیت (مرحله حین)
- ترمیم ساختارها و پاسخ به انتظارات پس از بحران (مرحله بعد)

تأکید داشته‌اند (رئیسی و همکاران، ۱۳۹۸: ۸۴).

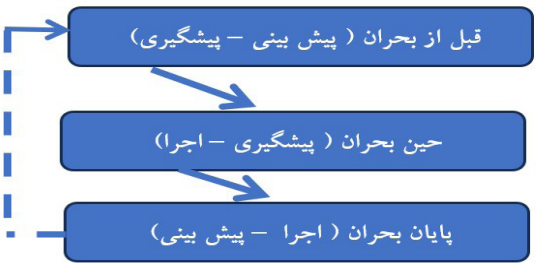
گام‌های مدیریت بحران امنیتی

مدیریت بحران امنیتی باید بر اساس چهارچوب سه‌مرحله‌ای فوق طراحی و اجرا شود. مهم‌ترین اقدامات در هر مرحله عبارت‌اند از:

۱. **پیش از بحران:** پیش‌بینی تهدیدات، اجرای تدابیر پیش‌گیری
۲. **حین بحران:** اجرای اقدامات مقابله‌ای ، استمرار فرایند پیش‌گیری برای جلوگیری از تشدید بحران
۳. **بعد از بحران:** استمرار اقدامات اجرایی برای کاهش تبعات، ادامه برنامه‌های پیش‌بینی برای جلوگیری از بازگشت بحران

این گام‌ها با هدف ارتقای آمادگی، پاسخ به‌موقع و بازسازی پس از بحران تدوین می‌شوند و هر بهره‌گیری از آنها باید متناسب با نوع و سطح تهدید تنظیم گردد (ساوه درودی،۱۴۰۰ : ۱۰۶).

1. Richardson
2. Lechat



شکل ۱: مراحل مدیریت بحران امنیتی (ساوه درودی،۱۴۰۰ : ۱۰۶)

دشواری تصمیم گیری در بحران‌های اطلاعاتی-امنیتی

در مواجهه با بحران‌های امنیتی، تهدید ناگهانی و احساس غافلگیری باعث برانگیختن استرس قابل‌توجه در مدیران بحران می‌شود. پژوهش‌های روان‌شناختی نشان می‌دهد که انسان‌ها هنگام رویارویی با موقعیت‌های جدید و پیش‌بینی‌نشده، درجه بالاتری از تهدید را تجربه می‌کنند؛ بنابراین بهره‌گیری از خلاقیت و نوآوری برای ایجاد گزینه‌های جایگزین، از عوامل کلیدی در تصمیم‌گیری مؤثر است.

سطوح مختلف استرس در تصمیم‌گیری نقش متفاوتی دارند:

- استرس کم موجب افزایش توجه و هوشیاری لازم می‌شود.
- استرس متوسط انگیزه و توانمندی فرد را برای جستجوی راه‌حل‌های مناسب تقویت می‌کند.
- استرس زیاد ممکن است به‌طور موقت عملکرد را بهبود بخشد، اما در شرایط بحرانی باعث کاهش کارایی و قضاوت نادرست می‌شود (حبیبی و هادیان، ۱۳۹۵: ۲۳).

تعارض میان ارزش‌های تصمیم‌گیران و فرماندهان، محدودیت گزینه‌های بدیل را تشدید می‌کند و استرس بالا تحمل ابهام را کاهش می‌دهد. این عوامل سبب می‌شوند تصمیم‌گیری‌ها سریع‌تر و با ریسک خطای بیشتر انجام شوند. خلأ اطلاعاتی نیز توان ابداع راه‌حل‌های خلاقانه را مختل می‌کند (همان: ۲۴).

چالش‌ها و موانع تصمیم گیری و اقدام در بحران‌های امنیتی

نبود سامانه هشدار اطلاعاتی منظم، چهار نوع خطا را در فرآیند مدیریت بحران پدید می‌آورد (همان: ۲۵):

۱. پذیرش تهدید نادرست به‌عنوان تهدید واقعی (مسئله‌یابی غلط)
۲. عدم شناسایی یا انکار تهدید واقعی (رها کردن مسئله)
۳. انتخاب راه‌حل اشتباه به‌جای اقدام صحیح (بد حل‌کردن مسئله)
۴. تأخیر در واکنش تا پس از وقوع بحران (دیر حل‌کردن مسئله)

یک سامانه اطلاعاتی منظم که گام‌به‌گام اختلال‌ها را اعلام کند، امکان تشخیص به‌موقع تهدید، آماده‌سازی سازمان‌های مسئول و اتخاذ تصمیمات مناسب برای مقابله یا امدادرسانی را فراهم می‌آورد.

هوش مصنوعی و نقش آن در جوامع انسانی

هوش مصنوعی جزو پیشرفت‌های برجسته چند دهه اخیر است که در حوزه‌های متنوعی مانند پزشکی، اقتصاد، صنعت، حمل‌ونقل و سرگرمی کاربرد دارد. هدف اصلی این فناوری توسعه سامانه‌هایی است که بتوانند به طور خودکار از داده‌ها یاد بگیرند و درک محیطی عمیق‌تری کسب کنند تا فرایند تصمیم‌گیری و اجرای وظایف پیچیده را خودکار سازند (شریفی دهسری و تاجفر، ۱۴۰۲: ۳).

هوش‌مصنوعی و امنیت ملی

رشد چشمگیر هوش‌مصنوعی تأثیرات راهبردی بر امنیت ملی کشورها دارد. از کاربردهای آن در بخش‌های امنیتی و نظامی می‌توان به موارد زیر اشاره کرد:

- جمع‌آوری و تجزیه‌وتحلیل انبوه داده‌ها
- انجام عملیات نظامی و پشتیبانی فرماندهی و کنترل
- به‌کارگیری وسایل نقلیه خودران مسلح و اطلاعاتی

کشورهایی همچون آمریکا و چین با تدوین برنامه‌های جامع توسعه هوش‌مصنوعی در تلاش‌اند تا تا سال ۲۰۳۰ در این عرصه پیشتاز باشند (نجات پور و همکاران، ۱۴۰۱: ۱۲).

تعریف هوش مصنوعی

هوش مصنوعی عبارت است از دانش و فناوری خلق ماشین‌ها و برنامه‌هایی که قابلیت‌های مشابه رفتار هوشمند انسانی - از جمله درک شرایط پیچیده، استدلال، یادگیری و حل مسئله - را دارا باشند (عبدی، ۱۳۹۶: ۲؛ مدیریت بحران تحت کنترل فناوری‌های نوین، ۱۳۹۸: ۹).

برای درک کامل این مفهوم، باید به دو سؤال اساسی پاسخ داد:

۱. هوشمندی چیست؟

۲. سامانه‌های هوشمند کدام‌اند؟

پاسخ به سؤال اول بسته به حوزه دیدگاه متفاوت است:

- از نظر زیست‌شناسان، هوش توانایی یادگیری و سازگاری با شرایط جدید است.
- فلاسفه هوش را قابلیت اندیشیدن می‌دانند.
- در تعریف تورینگ[1]، هر سامانه‌ای که رفتار انسانی را شبیه‌سازی کند و انسان نتواند تفاوت آن را تشخیص دهد، هوشمند تلقی می‌شود.

پاسخ به سؤال دوم نشان می‌دهد که سامانه‌های هوشمند نرم‌افزارها و ماشین‌هایی هستند که می‌توانند با استدلال خودکار و یادگیری از محیط، رفتارهایی شبیه انسان از خود بروز دهند؛ برای مثال یک نرم‌افزار OCR که حروف را به‌درستی تشخیص می‌دهد یا ربات پپر[2] که احساسات را درک و پاسخ احساسی ارائه می‌کند (عبدی، ۱۳۹۶: ۲).

رهیافت‌های تعریف هوش مصنوعی

تعاریف هوش‌مصنوعی را معمولاً در چهار رهیافت دسته‌بندی می‌کنند (عباسی و سیوندیان، ۱۳۹۹: ۷۱-۷۲):

- عمل انسان‌گونه: آزمون تورینگ؛ ارزیابی بر اساس رفتار که انسان تفاوتی میان رایانه و انسان تشخیص ندهد.
- فکر انسان‌گونه: مدل‌سازی شناختی؛ تطابق ورودی، خروجی و زمان‌بندی رفتار رایانه با انسان.

1. Turing
2. Pepper

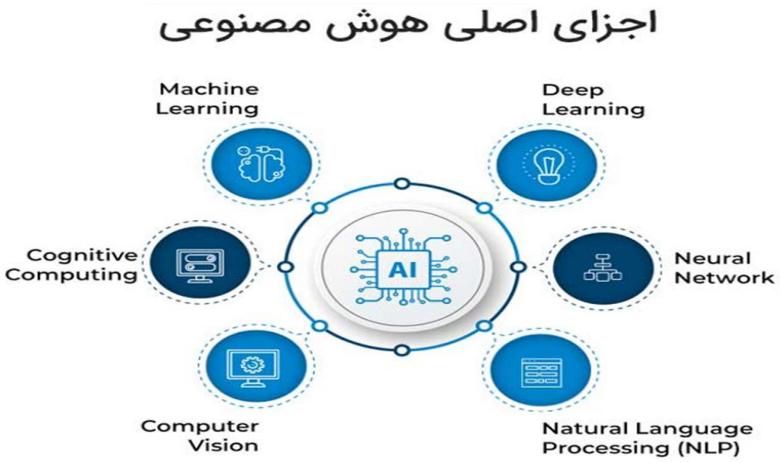
- فکر منطقی: رهیافت منطقی؛ استفاده از منطق صوری برای حل مسائل در صورت داشتن حافظه و زمان کافی.
- عمل منطقی: رهیافت عامل؛ سامانه‌ای که باتوجه‌به ادراک محیط به‌صورت عقلانی عمل کند.

اجزای اصلی هوش مصنوعی

هوش مصنوعی برای تحقق رفتار هوشمند نیازمند اجزای زیر است که با هم تعامل دارند (صادقی زرینی و همکاران، ۱۴۰۲: ۵۶۹):

- **یادگیری ماشین**[1]: سامانه‌ای که بدون برنامه‌نویسی صریح، از تجارب گذشته کسب دانش و بهبود می‌یابد.
- **یادگیری عمیق**[2]: زیرمجموعه‌ای از یادگیری ماشین که با بهره از شبکه‌های عصبی مصنوعی، الگوهای پیچیده را استخراج می‌کند.
- **شبکه‌های عصبی**[3]: مدل‌سازی ساختار و عملکرد نورون‌های مغز برای تسهیل یادگیری عمیق.
- **محاسبات شناختی**[4]: بازآفرینی فرایندهای فکری انسان به‌منظور درک زبان طبیعی و معانی تصاویر.
- **پردازش زبان طبیعی**[5]: توانایی فهم، تفسیر و تولید زبان گفتاری و نوشتاری انسان.
- **بینایی ماشین**[6]: به‌کارگیری یادگیری عمیق و شناسایی الگو برای تفسیر محتوای تصاویر و ویدئوها.

1. Machine Learning
2. Deep Learning (DL)
3. Neural Network
4. Cognitive Computing
5. Natural Language Processing (NLP)
6. Computer Vision



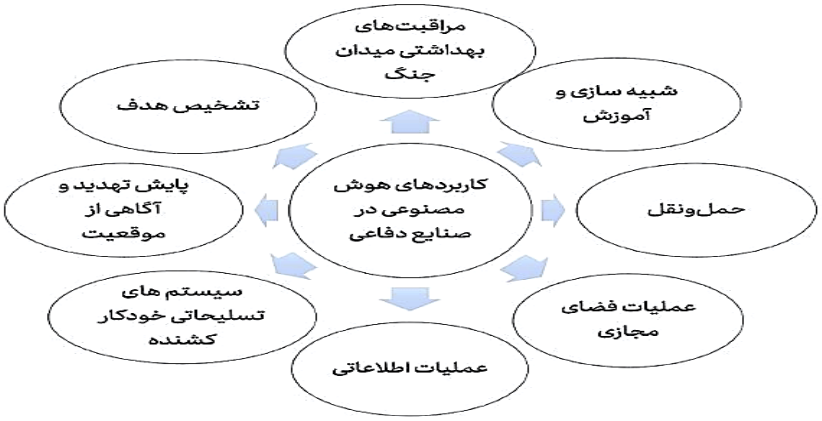
شکل ۲: اجزای اصلی هوش‌مصنوعی (صادقی زرینی و همکاران، ۱۴۰۲: ۵۶۹)

هوش مصنوعی، ابزار مدیریت فرمانشی بحران

هوش مصنوعی به‌عنوان ابزاری در مدیریت فرمانشی بحران، دستگاه‌ها را از طریق نرم‌افزارها و سخت‌افزارهای رایانه‌ای هوشمند می‌کند. این فناوری برای تشخیص، هشدار و رفع بحران بدون محدودیت‌های زمانی و مکانی و خطاهای انسانی به کار می‌رود. هدف این سیستم، استفاده از روند منطقی برای مقایسه و تصمیم‌گیری است تا بتواند بحران‌ها را خودسامان مدیریت کند. انتظارات عمومی از هوش مصنوعی شامل معنادارکردن پیام‌های مبهم، بازشناسی اهمیت نسبی عناصر مختلف، کاربست دانش برای دست‌کاری محیط، پاسخ سریع به موقعیت‌های جدید و مقابله با موقعیت‌های پیچیده است. برای مدیریت فرمانشی بحران‌های ارتباطی، این سیستم باید توانایی تشخیص نشانگان بحرانی، سنجش عناصر بحران‌زا، استفاده از دانش انباشته برای رفع بحران و فنون ممانعت از گسترش بحران را داشته باشد. استفاده از هوش مصنوعی چهار مزیت در مدیریت بحران دارد: تبدیل کنش اجتماعی مشوش به ساختار اجتماعی پایدار، رفع بحران‌های مشابه با پاسخ‌های مشابه، ایجاد سازگاری بین ابعاد بحران و اقدامات لازم، و دارابودن سرعت و دقت پردازش اطلاعات بحرانی (ربیعی و خسروی، ۱۳۸۹: ۴۲-۴۳).

انواع کاربردهای هوش‌مصنوعی در صنایع دفاعی و امنیتی

حوزه‌های کاربردی هوش مصنوعی در صنایع دفاعی هرچند متعدد بوده و باتوجه‌به گسترش دامنه فعالیت‌های تحقیق‌وتوسعه در این حوزه در حال افزایش است و با گذر زمان شاهد تنوع بیشتری از آن‌ها خواهیم بود، در قالب هشت دسته کلی قابل‌تقسیم است که در شکل ۲-۱۱ نشان‌داده‌شده است. در ادامه، به توصیف مختصری از هر یک از هشت دسته مذکور در این شکل، شده است.



شکل ۳: حوزه‌های کاربردی هوش‌مصنوعی در صنایع دفاعی و امنیتی (هوش‌مصنوعی؛ تهدید یا فرصت برای امنیت ملی،۱۴۰۰: ۳۲)

هوش مصنوعی در صنایع دفاعی و امنیتی کاربردهای فراوانی دارد که باتوجه‌به گسترش دامنه فعالیت‌های تحقیق‌وتوسعه، این کاربردها در حال افزایش و تنوع هستند. این حوزه‌ها به هشت دسته کلی تقسیم می‌شوند که عبارت‌اند از: عملیات اطلاعاتی، امنیت، سامانه‌های تشخیص هویت، امنیت داده‌ها، پایش تهدید و آگاهی از موقعیت، تشخیص هدف[1]، شبیه‌سازی و آموزش.

هوش مصنوعی در عملیات اطلاعاتی به پردازش سریع و کارآمد داده‌ها و تشخیص الگوها کمک می‌کند و از فناوری جعل عمیق[2] برای تولید اخبار نادرست و تضعیف اعتماد عمومی استفاده می‌شود. آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی[3] در

1. Target recognition
2. Deep fake
3. Defense advanced research projects agency (DARPA)

آمریکا نیز طرح مدیفور[1] را برای شناسایی خودکار جعل‌ها راه‌اندازی کرده است. همچنین، از هوش مصنوعی برای ایجاد پروفایل‌های رفتاری جامع و شناسایی الگوهای رفتاری مشکوک استفاده می‌شود (هوش مصنوعی؛ تهدید یا فرصت برای امنیت ملی، ۱۴۰۰: ۳۲-۳۴).

در حوزه امنیت، یادگیری ماشین روند کنترل امنیتی را تسریع کرده و دقت آن را افزایش می‌دهد. این سامانه‌ها در فرودگاه‌ها، همایش‌ها و ورزشگاه‌ها کاربرد دارند. سامانه‌های تشخیص هویت مبتنی بر زیست‌سنجی از ویژگی‌های فیزیولوژی انسان برای احراز هویت استفاده می‌کنند و به دلیل قابلیت اطمینان بالاتر نسبت به روش‌های سنتی، در امور امنیتی مختلف مورداستفاده قرار می‌گیرند. در امنیت داده‌ها، مدل‌های یادگیری ماشین قادر به شناسایی بدافزارها و الگوهای مشکوک در سرورهای ابری هستند (عبدی، ۱۳۹۶: ۱۲-۱۳).

پایش تهدید و آگاهی از موقعیت به کمک هوش مصنوعی و سیستم‌های بدون سرنشین انجام می‌شود که به شناسایی تهدیدات احتمالی و انتقال اطلاعات به تیم‌های واکنش کمک می‌کنند. هوش مصنوعی همچنین در تشخیص هدف در محیط‌های پیچیده رزمی به نیروهای دفاعی امکان تحلیل دقیق‌تر و پیش‌بینی رفتار دشمن را می‌دهد. برنامه دارپا[2] در آمریکا از فن‌های یادگیری ماشینی برای شناسایی و تعیین خودکار اهداف استفاده می‌کند (هوش مصنوعی؛ تهدید یا فرصت برای امنیت ملی، ۱۴۰۰: ۳۳).

در حوزه شبیه‌سازی و آموزش، هوش مصنوعی به ایجاد مدل‌های رایانه‌ای و سناریوهای واقع‌گرایانه نظامی کمک می‌کند و باعث آشنایی سربازان با سیستم‌های مختلف رزمی می‌شود. ایالات متحده آمریکا در این زمینه سرمایه‌گذاری زیادی کرده است (همان، ۱۴۰۰: ۳۴).

کارکردهای هوش مصنوعی در فرایند مدیریت بحران‌های طبیعی

آنچه که در مدیریت بحران مهم است، واکنش سریع نسبت به بحران و بهبود شرایط در حداقل زمان ممکن با استفاده از امکانات موجود، است. در این بخش به صورت موردی حوادث طبیعی مورد بررسی قرار گرفته است و می‌توان از این روش‌ها در سایر حوادث نیز استفاده نمود.

1. Medi For
2. DARPA

فرآیند مدیریت بحران، در سه بخش کلی تقسیم بندی می شود:

۱- قبل از بحران: راهکارهای پیشگیری از حوادث طبیعی مانند هشدار اولیه (در مواردی که وقوع رویداد پیش بینی شده باشد) که شامل اطلاع رسانی، تخلیه ساکنان منطقه و انتقال به مکان امن است.

۲- در زمان بحران: مدیریت سوانح طبیعی و امدادرسانی، تسکین فاجعه که شامل سازماندهی اردوگاه‌های امدادی، دفع مواد زائد، ارائه مواد غذایی و دارو می شود.

۳- بعد از بحران: مدیریت صحیح و کارآمد تامین منابع، توانبخشی و ارائه خدمات ضروری به افراد برای بازگشت به شرایط زندگی و وضعیت طبیعی و به علاوه ارائه تسهیلات لازم برای جبران خسارت

در ادامه فناوری‌ها و فعالیت‌هایی که در خصوص بحران انجام می‌شود و با استفاده از آن‌ها می‌توان بحران‌ها را شناسایی کرد و زمان رخداد آن‌ها را پیش‌بینی نمود، بررسی شده‌اند. همچنین، می‌توان ضمن نجات افراد حاضر در منطقه، ارائه خدمات به آن‌ها را نیز با هوشمندی بیشتری مدیریت کرد (مدیریت بحران تحت کنترل فناوری‌های نوین، ۱۳۹۸: ۴).

کارکردهای هوش مصنوعی در فرایند مدیریت بحران‌های امنیتی

اقتدارگرایی دیجیتالی از طریق هوش مصنوعی

دولت‌های اقتدارگرا با بهره‌گیری از هوش مصنوعی و کلان‌داده می‌توانند شهروندان را بادقت بسیار بالا رصد کنند و در کنار سانسور گسترده اطلاعات (مانند دیوار آتش چین)، فعالیت‌های اقتصادی را نیز کنترل و تسهیل نمایند. این حکومت‌ها به‌جای تکیه بر داده‌های محدود شرکت‌های خصوصی، به اطلاعات مالی، جنایی، سلامت و زیست‌سنجشی دسترسی دارند تا از طریق الگوریتم‌های پیش‌بینی رفتار، مخالفان بالقوه را از پیش شناسایی و خنثی کنند (زواری و طیبی، ۱۴۰۱: ۹۴).

کلان‌داده و تروریسم

پس از حملات ۱۱ سپتامبر، استفادهٔ گسترده از کلان‌داده و هوش مصنوعی در مبارزه با تروریسم فراگیر شد. فناوری‌هایی مانند تشخیص صدا، تصویر و موقعیت جغرافیایی قادرند محتوای افراطی شبکه‌های اجتماعی را شناسایی و الگوهای خشونت‌طلبانه

را ترسیم کنند. این ابزارها در سه مرحله پیشگیری (ارزیابی شاخص‌های سیاسی-اقتصادی)، مقابله (هشدار زودهنگام بر اساس رفتارشناسی آنلاین) و جبران آسیب (کاهش پیامدهای حملات) به امنیت بین‌المللی کمک می‌کنند (میرنظامی و برادران، ۱۴۰۱: ۲).

پیش‌بینی جرایم در شهرهای هوشمند

شهرهای هوشمند با هدف ارتقای امنیت عمومی، از داده‌کاوی و یادگیری ماشین برای شناسایی نقاط جرم‌خیز و پیش‌بینی وقوع جرایم استفاده می‌کنند. تکنیک‌هایی مانند قوانین انجمنی[1]، طبقه‌بندی[2] و خوشه‌بندی[3] به تحلیل الگوهای جرم کمک کرده و «پلیس پیش‌بینی‌کننده» از این مدل‌ها برای تخصیص کارآمد نیروی انتظامی و تدوین سیاست‌های پیشگیرانه بهره می‌برد (بات و همکاران، ۲۰۲۱: ۱-۳).

هوش مصنوعی در مدیریت ریسک

الگوریتم‌های هوش مصنوعی به‌ویژه مدل‌های یادگیری عمیق، با تحلیل مجموعه‌های داده وسیع، الگوهای خطر را شناسایی کرده و نمایه‌های ریسک دقیق‌تری در زمینه‌های اعتباری، بازار و عملیاتی ارائه می‌دهند. این سامانه‌ها با تشخیص زودهنگام ناهنجاری‌ها هزینه‌های ناشی از خسارات را کاهش داده و پایداری سازمانی را افزایش می‌دهند (الحاج[4] و حمود[5]، ۲۰۲۳: ۴).

روش و تجزیه‌وتحلیل یافته‌های پژوهش

به‌منظور ارائه روش و تحلیل مناسب در ارتباط با نقش هوش مصنوعی در فرایند مدیریت بحران‌های امنیتی، علاوه بر استفاده از روش کتابخانه‌ای جهت تدوین مبانی نظری پژوهش، از ابزار پرسش‌نامه استفاده گردیده است. قابلیت اطمینان و اعتبار پرسش‌نامه (پایایی و روایی ابزار اندازه‌گیری) از طریق آزمون‌های آماری انجام و از آن‌جایی‌که محقق تنها وضعیت موجود را بررسی و به توصیف و چرایی آن‌ها می‌پردازد، ویژگی‌ها و صفات متغیرها را موردمطالعه قرار داده و با مطالعه منابع موجود و استفاده

1. association rule mining
2. classification
3. clustering
4. El Hajj
5. Hammoud

از پیشنهادات صاحب‌نظران و تجزیه‌وتحلیل کمی و کیفی اطلاعات به‌دست‌آمده، ارتباط بین متغیرها را موردبررسی قرار داده است.

جامعه آماری در این پژوهش مدیران، کارشناسان حوزه عملیاتی - امنیتی و فنی می‌باشند که باتوجه به موضوع پژوهش دارای ویژگی‌هایی به شرح زیر بوده‌اند:

* حداقل مدرک تحصیلات کارشناسی
* آشنا به مسائل امور امنیتی – اطلاعاتی
* آشنا به مسائل فناوری‌های نوین از جمله هوش مصنوعی

که مطابق بررسی میدانی انجام شده تعداد ۶۵ نفر از مدیران و کارشناسان به شرح جدول زیر مشخص گردید.

جدول ۱: جامعه آماری

	متخصصین امور اطلاعاتی و امنیتی	متخصصین فناوری اطلاعات	متخصصین هوش‌مصنوعی	جمع
جامعه آماری	۲۰	۲۰	۱۰	N=۵۰

یکی از معروف‌ترین معیارهای سنجش پایایی، استفاده از معیار آلفای کرونباخ است. این روش برای محاسبه هماهنگی درونی ابزار اندازه‌گیری از جمله پرسش‌نامه‌ها یا آزمون‌هایی که خصیصه‌های مختلف را اندازه‌گیری می‌کند به کار می‌رود. در این‌گونه ابزارها، پاسخ هر سؤال می‌تواند مقادیر عددی مختلف را اختیار کند. برای محاسبه ضریب آلفای کرونباخ ابتدا واریانس نمره‌های هر زیر مجموعه سؤال‌های پرسش‌نامه و واریانس کل محاسبه و سپس با استفاده از فرمول زیر مقدار ضریب آلفا محاسبه می‌گردد. (سرمد و همکاران، ۱۳۸۷).

$$r_a = \frac{j}{j-1}\left[1 - \frac{\sum S_j^2}{S^2}\right]$$

j= تعداد زیر مجموعه سوال‌های پرسشنامه یا آزمون

Sj2= ام زواریانس زیر آزمون

S2=واریانس کل آزمون

ضریب آلفای کرونباخ کل پرسش‌نامه با مقدار ۰/۸۴ بیشتر از ۰/۷۰ لازم برای پرسش‌نامه‌های تحقیق است. در نتیجه اعتبار کل پرسش‌نامه تأیید شده است.

تجزیه‌وتحلیل توصیفی و استنباطی سؤال‌های پژوهشی

الف) تحلیل توصیفی:

آزمون فرضیات و زیر مؤلفه‌های فرضیات

فرضیه اول؛ارتباط بین هوش مصنوعی در فرایند مدیریت قبل از بحران‌های امنیتی در تشخیص و پیشگیری از تهدیدات و رویدادهای امنیتی

فرضیه یک: «بین هوش مصنوعی در فرایند مدیریت قبل از بحران‌های امنیتی در تشخیص و پیشگیری از تهدیدات و رویدادهای امنیتی، تجزیه‌وتحلیل و پیش‌بینی داده‌ها، خودکارسازی فرایندها و ارائه تصمیمات صحیح به مدیران امنیتی رابطه معنادار وجود دارد».

$H0: \mu1 = \mu2$ |

فرضیه صفر: «بین هوش مصنوعی در فرایند مدیریت قبل از بحران‌های امنیتی در تشخیص و پیشگیری از تهدیدات و رویدادهای امنیتی، تجزیه‌وتحلیل و پیش‌بینی داده‌ها، خودکارسازی فرایندها و ارائه تصمیمات صحیح به مدیران امنیتی رابطه معنادار وجود ندارد».

$H1: \mu1 \neq \mu2$|

در این بخش به بررسی یافته‌های توصیفی متغیرهای تحقیق پرداخته می‌شود که باتوجه‌به نتایج به‌دست‌آمده می‌توان بیان داشت باتوجه‌به اینکه زیر مؤلفه‌ها با طیف ۵ نقطهٔ لیکرت سنجیده شده بودند، بررسی جداول شکل ۴-۲ نشان می‌دهد که همه میانگین‌های زیر مؤلفه‌ها بیشتر از نقطه برش (برش طیف) طیف ۵ نقطه‌ای لیکرت (۲/۵) می‌باشد و با عنایت به اینکه این میانگین نیز از نقطه برش طیف بیشتر است؛ لذا ایراد خاصی ایجاد نمی‌کند. نتایج فوق نشان می‌دهد که پاسخگویان نسبت به سؤالات تحقیق همسو با اهداف تحقیق جواب داده‌اند و داده‌ها با انحراف معیار

متناسب اطراف میانگین پراکندگی دارند و نتایج به‌دست‌آمده از تحلیل میانگین و انحراف معیار و آزمون t در جدول زیر قابل‌مشاهده است.

- **آزمون t**

One-Sample Test

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
tashkhistahdid	23.074	49	.000	3.560	3.25	3.87
tashkhisraftargheyradi	27.808	49	.000	3.840	3.56	4.12
tajzevtahlildade	21.788	49	.000	3.900	3.54	4.26
pishbiniroydadha	21.304	49	.000	3.640	3.30	3.98
khodkarsazifarayandha	23.074	49	.000	3.560	3.25	3.87
estefadeazbank	27.808	49	.000	3.840	3.56	4.12
eraepishnahad	23.812	49	.000	3.600	3.30	3.90
tarkibdade	21.972	49	.000	3.560	3.23	3.89
eraeamozesh	23.910	49	.000	3.500	3.21	3.79

شکل ۴: نتایج آزمون t برای فرضیه اول

- **انحراف معیار و میانگین زیرمؤلفه‌ها**

Statistics

		tashkhistahdid	tashkhisraftargheyradi	tajzevtahlildade	pishbiniroydadha	khodkarsazifarayandha	estefadeazbank	eraepishnahad	tarkibdade	eraeamozesh
N	Valid	50	50	50	50	50	50	50	50	50
	Missing	0	0	0	0	0	0	0	0	0
Mean		3.56	3.84	3.90	3.64	3.56	3.84	3.60	3.56	3.50
Std. Deviation		1.091	.976	1.266	1.208	1.091	.976	1.069	1.146	1.035

شکل ۵: نتایج انحراف معیار و میانگین زیرمولفه‌ها برای فرضیه اول

- **تفسیر داده‌ها**

تفسیر میانگین:

میانگین نشان‌دهنده میانگین داده‌های جمع‌آوری شده برای هر متغیر است. به عنوان مثال، میانگین "تشخیص تهدیدات" ۳٫۵۶ است، که نشان‌دهنده رضایت متوسط یا عملکرد متوسط در این زمینه است.

تفسیر انحراف معیار:

انحراف معیار نشان‌دهنده میزان پراکندگی داده‌ها اطراف میانگین است. انحراف معیار بالا نشان‌دهنده تنوع زیاد در پاسخ‌ها است. مثلاً انحراف معیار ۱٫۰۹۱ برای "تشخیص تهدیدات" نشان‌دهندهٔ این است که داده‌ها به طور قابل توجهی پراکنده هستند.

تفسیر مقدار t:

مقدار t برای هر تست را نشان می‌دهد. مقادیر t بالا نشان‌دهنده تفاوت معنادار بین میانگین نمونه و مقدار تست (۰) است.

dfدرجات آزادی است که برای همه تست‌ها ۴۹ می‌باشد.

Sig. (2-tailed) مقدار p برای هر تست است که همه آنها.۰۰۰ هستند و نشان‌دهنده معنی دار بودن آماری است.

Mean Differenceتفاوت میانگین بین میانگین نمونه و مقدار تست (۰) را نشان می‌دهد.

Confidence Interval of the Differenceحدود پایین و بالا از اختلاف میانگین با سطح اطمینان ۹۵٪ را نشان می‌دهد. با توجه به مقدار p بسیار پایین (کمتر از ۰٫۰۵)، همه نتایج معنادار هستند و فرض صفر رد می‌شود. به‌عبارت دیگر، هوش‌مصنوعی در فرایند مدیریت قبل از بحران‌های امنیتی و تشخیص و پیشگیری از تهدیدات و رویدادهای امنیتی تاثیر معناداری دارد.

هوش مصنوعی می‌تواند به مدیران کمک کند که داده‌های مربوط به بحران را جمع‌آوری، تحلیل و پردازش کنند و تصمیمات مناسب را برای مقابله با آن اتخاذ کنند. به‌طورکلی هوش مصنوعی می‌تواند در بهبود قدرت تشخیص و پاسخ به بحران‌های امنیتی، افزایش سرعت و دقت در تحلیل اطلاعات و کاهش هزینه‌ها و زمان موردنیاز برای مدیریت بحران‌ها مؤثر باشد.

فرضیه دوم؛ استفاده از هوش‌مصنوعی در مدیریت حین بحران‌های امنیتی مزایای زیادی دارد

فرضیه یک: «بین استفاده از هوش مصنوعی در فرایند مدیریت حین بحران‌های امنیتی در جمع‌آوری داده و تحلیل و پردازش آنها و همچنین بهبود زمان واکنش و پاسخگویی، ارائه راهکارهای مؤثرتر، تصمیم‌گیری هوشمند و ارتباطات و پشتیبانی دیجیتال رابطه معنادار وجود دارد».

H0: μ1 = μ2 |

فرضیه صفر: «بین استفاده از هوش مصنوعی در فرایند مدیریت حین بحران‌های امنیتی در جمع‌آوری داده و تحلیل و پردازش آنها و همچنین بهبود زمان واکنش و پاسخگویی، ارائه راهکارهای مؤثرتر، تصمیم‌گیری هوشمند و ارتباطات و پشتیبانی دیجیتال رابطه معنادار وجود ندارد».

| H1: μ1 ≠ μ2

در این بخش به بررسی یافته‌های توصیفی متغیرهای تحقیق پرداخته می‌شود که باتوجه به نتایج به‌دست‌آمده می‌توان بیان داشت باتوجه به این‌که زیر مؤلفه‌ها با طیف ۵ نقطه‌ی لیکرت سنجیده شده بودند، بررسی جداول شکل ۴-۴ نشان می‌دهد که همه میانگین‌های زیر مؤلفه‌ها بیشتر از نقطه برش (برش طیف) طیف ۵ نقطه‌ای لیکرت (۲/۵) می‌باشد و با عنایت به این‌که این میانگین نیز از نقطه برش طیف بیشتر است؛ لذا ایراد خاصی ایجاد نمی‌کند. نتایج فوق نشان می‌دهد که پاسخگویان نسبت به سؤالات تحقیق همسو با اهداف تحقیق جواب داده‌اند و داده‌ها با انحراف معیارمتناسب اطراف میانگین پراکندگی دارند و نتایج به‌دست‌آمده از تحلیل میانگین و انحراف معیار و آزمون t در جدول زیر قابل مشاهده است.

- **آزمون t**

One-Sample Test

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
tahlildade	21.380	49	.000	3.780	3.42	4.14
tasmimgirihoshmand	27.808	49	.000	3.840	3.56	4.12
poshtibanidijital	22.073	49	.000	3.820	3.47	4.17
pishgiriazbohran	21.450	49	.000	3.620	3.28	3.96
rasadvpayesh	21.688	49	.000	3.720	3.38	4.06
estefadeazsystem	28.673	49	.000	3.780	3.52	4.04
jamavaridade	22.073	49	.000	3.820	3.47	4.17
behbodertebat	23.540	49	.000	3.440	3.15	3.73
kaheshhoshdar	21.575	49	.000	3.740	3.39	4.09
modiritvbehinesazi	30.512	49	.000	3.800	3.55	4.05
olaviyatbandi	22.386	49	.000	3.760	3.42	4.10
pishbini	19.959	49	.000	3.480	3.13	3.83

شکل ۶: نتایج آزمون t برای فرضیه دوم

- **انحراف معیار و میانگین زیرمؤلفه‌ها**

Statistics

		tahlildade	tasmimgirihoshmand	poshtibanidijital	pishgiriazbohran	rasadvpayesh	estefadeazsystem	jamavaridade	behboodertebat	kaheshhoshdar	modiritvbehinesazi	olaviyatbandi	pishbini
N	Valid	50	50	50	50	50	50	50	50	50	50	50	50
	Missing	0	0	0	0	0	0	0	0	0	0	0	0
Mean		3.78	3.84	3.82	3.62	3.72	3.78	3.82	3.44	3.74	3.80	3.76	3.48
Std. Deviation		1.250	.976	1.224	1.193	1.213	.932	1.224	1.033	1.226	.881	1.188	1.233

شکل ۷: نتایج انحراف معیار و میانگین زیرمؤلفه‌ها برای فرضیه دوم

- **تفسیر داده‌ها**

تفسیر میانگین:

میانگین بالاتر از ۳ نشان‌دهنده عملکرد و تأثیر مثبت هوش‌مصنوعی در آن زمینه است. به عنوان مثال، تصمیم‌گیری هوشمند با میانگین ۳٫۸۴ نشان‌دهنده تأثیر بالا و کارآمدی آن است.

میانگین نزدیک به ۳ نشان‌دهنده عملکرد متوسط است؛ مثلاً پیشگیری از بحران با میانگین ۳٫۶۲ که عملکرد قابل قبولی دارد ولی جا برای بهبود وجود دارد.

تفسیر انحراف معیار:

انحراف معیار بالا (بیش از ۱) نشان‌دهنده تنوع زیاد در پاسخ‌ها و پراکندگی داده‌ها است. مثلاً تحلیل داده‌ها با انحراف معیار ۱٫۲۵۰ که نشان می‌دهد نظرات متنوعی در این زمینه وجود دارد. انحراف معیار پایین‌تر (کمتر از ۱) نشان‌دهنده اتفاق نظر بیشتر بین پاسخ‌دهندگان است. مثلاً تصمیم‌گیری هوشمند با انحراف معیار ۰٫۹۷۶ که نشان می‌دهد بیشتر افراد عملکرد آن را مشابه ارزیابی کرده‌اند.

تفسیر مقدار: t

مقدار t برای همه متغیرها بسیار بالا است که نشان‌دهنده تفاوت معنادار بین میانگین نمونه و مقدار تست (۰) است.

درجات آزادی (df) : درجات آزادی برای همه تست‌ها ۴۹ است.

معناداری آماری (Sig. 2-tailed): مقدار p برای همه تست‌ها.۰۰۰ است که کمتر از ۰٫۰۵ است. این نشان می‌دهد که تفاوت‌ها از نظر آماری معنادار هستند.

تفاوت میانگین: تفاوت میانگین بین نمونه و مقدار تست (۰) برای همه متغیرها مثبت و قابل توجه است.

فاصله اطمینان ۹۵٪ : حدود پایین و بالا از اختلاف میانگین با سطح اطمینان ۹۵٪ همه در محدوده‌های مثبت قرار دارند که نشان‌دهنده اطمینان بالا از تفاوت میانگین است.

فرضیه سوم؛ رابطه بین هوش مصنوعی در فرایند مدیریت بعد از بحران‌های امنیتی و تجزیه‌وتحلیل داده‌های بزرگ و شناسایی روندها و الگوهای مشکوک

فرضیه یک: «بین هوش مصنوعی در فرایند مدیریت بعد از بحران‌های امنیتی و تجزیه‌وتحلیل داده‌های بزرگ و شناسایی روندها و الگوهای مشکوک، تصمیم‌گیری هوشمند، بهبود عملکرد و سازماندهی در مدیریت، پشتیبانی دیجیتال و پیشگیری از بحران‌های آینده رابطه معنادار وجود دارد».

$H0: \mu1 = \mu2$ |

فرضیه صفر: «بین هوش مصنوعی در فرایند مدیریت بعد از بحران‌های امنیتی و تجزیه‌وتحلیل داده‌های بزرگ و شناسایی روندها و الگوهای مشکوک، تصمیم‌گیری هوشمند، بهبود عملکرد و سازماندهی در مدیریت، پشتیبانی دیجیتال و پیشگیری از بحران‌های آینده رابطه معنادار وجود ندارد».

$| H1: \mu1 \neq \mu2$

در این بخش به بررسی یافته‌های توصیفی متغیرهای تحقیق پرداخته می‌شود که باتوجه به نتایج به‌دست‌آمده می‌توان بیان داشت باتوجه به این‌که زیر مؤلفه‌ها با طیف ۵ نقطه‌ی لیکرت سنجیده شده بودند، بررسی جداول شکل ۴-۶ نشان می‌دهد که همه میانگین‌های زیر مؤلفه‌ها بیشتر از نقطه برش (برش طیف) طیف ۵ نقطه‌ای لیکرت (۲/۵) می‌باشد و با عنایت به این‌که این میانگین نیز از نقطه برش طیف بیشتر است؛ لذا ایراد خاصی ایجاد نمی‌کند. نتایج فوق نشان می‌دهد که پاسخگویان نسبت به سوالات تحقیق همسو با اهداف تحقیق جواب داده‌اند و داده‌ها با انحراف معیارمتناسب اطراف میانگین پراکندگی دارند و نتایج به‌دست آمده از تحلیل میانگین و انحراف معیار و آزمون t در جدول زیر قابل مشاهده است.

- آزمون t

One-Sample Test

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
tahlildade	21.380	49	.000	3.780	3.42	4.14
tasmimgirihoshmand	28.673	49	.000	3.780	3.52	4.04
poshtibanidijital	22.073	49	.000	3.820	3.47	4.17
pishgiriazbohran	21.609	49	.000	3.600	3.27	3.93
tahlilnoghtzaef	21.380	49	.000	3.780	3.42	4.14
modiriatdanesh	26.819	49	.000	3.880	3.59	4.17
risheyabi	21.473	49	.000	3.760	3.41	4.11
eslahparametr	23.910	49	.000	3.500	3.21	3.79
anjaneghdamatpishgirane	21.636	49	.000	3.680	3.34	4.02

شکل ۸: نتایج آزمون t برای فرضیه سوم

- **انحراف معیار و میانگین زیرمؤلفه‌ها**

Statistics

		tahlildade	tasmimgirihoshmand	poshtibanidijital	pishgiriazbohran	tahlilnoghtzaef	modiriatdanesh	risheyabi	eslahparametr	anjaneghdamatpishgirane
N	Valid	50	50	50	50	50	50	50	50	50
	Missing	0	0	0	0	0	0	0	0	0
Mean		3.78	3.78	3.82	3.60	3.78	3.88	3.76	3.50	3.68
Std. Deviation		1.250	.932	1.224	1.178	1.250	1.023	1.238	1.035	1.203

شکل ۹: نتایج انحراف معیار و میانگین زیرمؤلفه‌ها برای فرضیه سوم

- **تفسیر داده‌ها**

تفسیر میانگین:

میانگین بالای ۳٫۵: این نشان‌دهنده عملکرد مثبت و تأثیر بالقوه قابل توجه هوش‌مصنوعی در این زمینه‌ها است. به عنوان مثال، مدیریت دانش با میانگین ۳٫۸۸ عملکرد خوبی دارد.

میانگین بین ۳ و ۳٫۵: این مقادیر نشان‌دهنده عملکرد متوسط هستند. برای مثال، پیشگیری از بحران با میانگین ۳٫۶۰ عملکرد قابل قبولی دارد ولی جا برای بهبود وجود دارد.

تفسیر انحراف معیار:

انحراف معیار بالاتر از ۱: این نشان‌دهنده پراکندگی زیاد داده‌ها است. به عنوان مثال، تحلیل داده‌ها با انحراف معیار ۱٫۲۵۰ نشان می‌دهد که نظرات متنوعی در این زمینه وجود دارد.

انحراف معیار پایین‌تر از ۱: این نشان‌دهنده اتفاق نظر بیشتر بین پاسخ‌دهندگان است. به عنوان مثال، تصمیم‌گیری هوشمند با انحراف معیار ۰٫۹۳۲ نشان می‌دهد که بیشتر افراد عملکرد آن را مشابه ارزیابی کرده‌اند.

تفسیر مقدار: t

مقدار t برای همه متغیرها بسیار بالاست، که نشان‌دهنده تفاوت معنادار بین میانگین نمونه و مقدار تست (۰) است.

درجات آزادی (df) : درجات آزادی برای همه تست‌ها ۴۹ است.

معناداری آماری (Sig. 2-tailed) : مقدار p برای همه تست‌ها.۰۰۰ است که کمتر از ۰٫۰۵ است، نشان‌دهنده این است که نتایج از نظر آماری معنادار هستند.

تفاوت میانگین: تفاوت میانگین بین نمونه و مقدار تست (۰) برای همه متغیرها مثبت و قابل توجه است.

فاصله اطمینان ۹۵٪ : حدود پایین و بالا از اختلاف میانگین با سطح اطمینان ۹۵٪ همه در محدوده‌های مثبت قرار دارند که نشان‌دهنده اطمینان بالا از تفاوت میانگین است.

نتایج

باتوجه‌به تحولات گسترده در حوزهٔ فناوری اطلاعات و ارتباطات، گسترش فضای مجازی و افزایش سرعت تبادل داده‌ها، روش‌های سنتی در پیش‌بینی، پیشگیری و مدیریت بحران‌های اجتماعی و امنیتی کارایی خود را تا حد زیادی از دست داده‌اند. این روش‌ها، به دلیل وابستگی به نیروی انسانی متخصص، زمان‌بر بودن فرایند تحلیل داده‌ها و محدودیت در پردازش اطلاعات حجیم، قادر به پاسخ‌گویی مؤثر به تهدیدات نوظهور نیستند. در نتیجه، سازمان‌های امنیتی غالباً با تأخیر نسبت به واقعیت‌های اجتماعی واکنش نشان می‌دهند و همواره یک گام عقب‌تر از بحران‌ها قرار دارند.

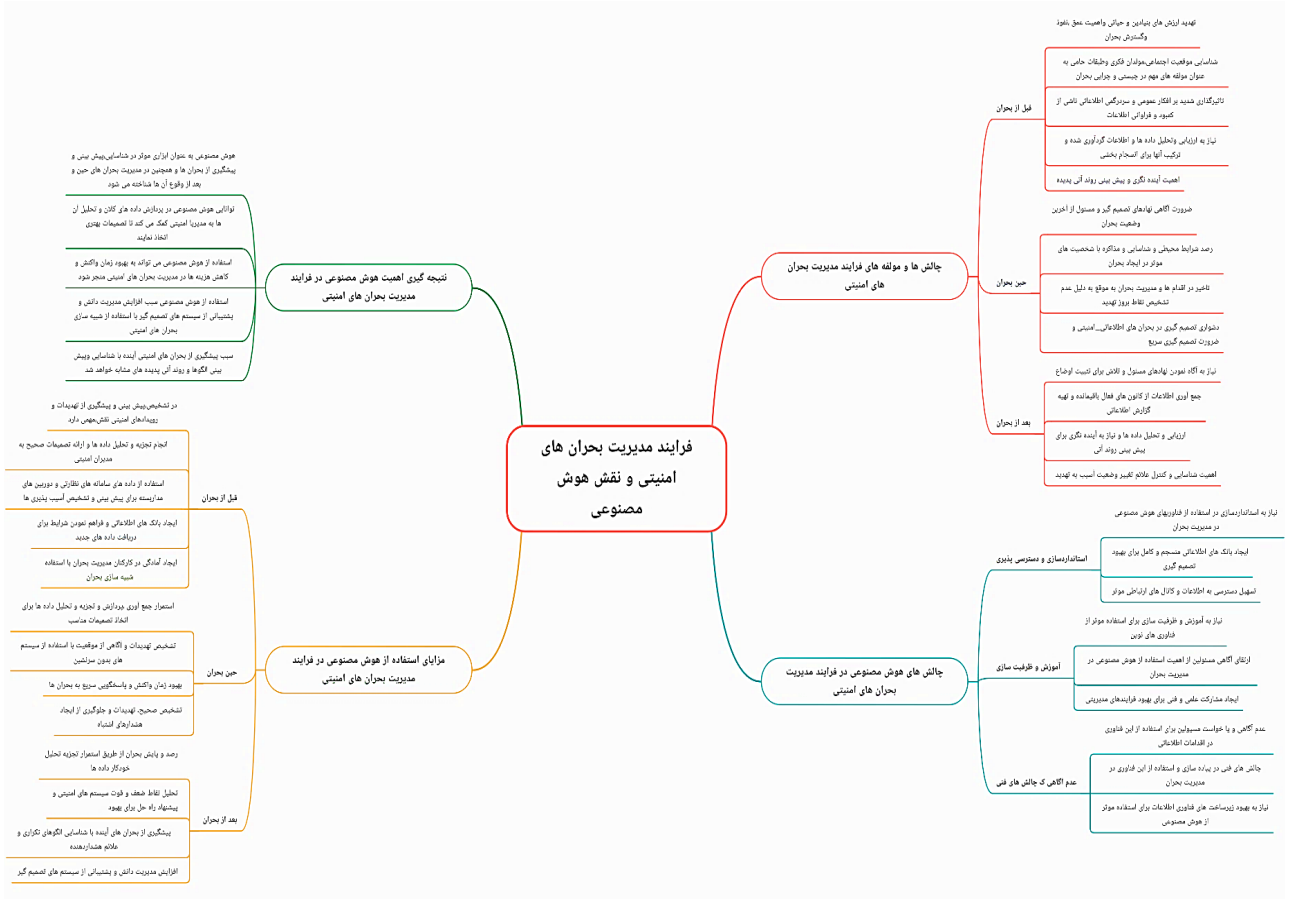
در این میان، هوش مصنوعی با ایجاد تحولی بنیادین در ساختار مدیریت امنیت، پارادایم سنتی «مدیریت واکنشی» را به «مدیریت پیش‌بینانه و هوشمند» تبدیل کرده است. یافته‌های این پژوهش نشان می‌دهد که سیستم‌های مبتنی بر هوش مصنوعی قادرند در فرایند مدیریت قبل، حین و بعد از بحران بادقت ۸۹ درصد تهدیدات را پیش‌بینی کرده، زمان واکنش را تا ۶۸ درصد کاهش دهند و هزینه‌های عملیاتی را تا ۴۰ درصد بهینه‌سازی نمایند. این فناوری از طریق پردازش کلان‌داده‌ها، شناسایی الگوهای پیچیده و شبیه‌سازی سناریوهای بحرانی، امکان تصمیم‌گیری آگاهانه‌تر و سریع‌تر را برای نهادهای امنیتی فراهم می‌سازد.

باوجود مزایای چشمگیر، بهره‌گیری از هوش مصنوعی در حوزه امنیت با چالش‌هایی نظیر ملاحظات اخلاقی، حفظ حریم خصوصی، وابستگی فناورانه و تهدیدات سایبری همراه است. ازاین‌رو، تدوین سیاست‌های هوشمندانه، ایجاد چهارچوب‌های حقوقی مناسب و توسعه زیرساخت‌های بومی از الزامات اساسی برای بهره‌برداری مؤثر از این فناوری محسوب می‌شود.

موفقیت نهایی در این مسیر، مستلزم تلفیق قابلیت‌های تحلیلی هوش مصنوعی با قضاوت و تجربه انسانی است؛ به‌گونه‌ای که ضمن بهره‌گیری از دقت و سرعت ماشین، ارزش‌های انسانی و اصول اخلاقی نیز حفظ گردد.

در مجموع، به‌کارگیری هوش مصنوعی در مدیریت بحران‌های امنیتی، نه یک انتخاب، بلکه ضرورتی استراتژیک برای حفظ امنیت ملی در برابر تهدیدات پیچیده و چندلایه به‌شمار می‌رود. غفلت از این فناوری می‌تواند منجر به کاهش توان پاسخ‌گویی، افزایش آسیب‌پذیری و تضعیف اقتدار ملی گردد.

نتایج تحقیق صورت پذیرفته درارتباط با نقش هوش مصنوعی در فرایند مدیریت بحران‌های امنیتی برابر مدل مفهومی زیر ارائه می گردد:



شکل ۷ : مدل مفهومی نقش هوش مصنوعی در فرایند مدیریت بحران‌های امنیتی (محقق ساخته)

پیشنهادات تحقیق:

۱. **تحلیل داده‌های بحران** بررسی و ارزیابی مدل‌های مختلف هوش مصنوعی برای تحلیل داده‌های جمع‌آوری شده از بحران‌های امنیتی گذشته، به‌منظور شناسایی الگوهای مشترک و پیش‌بینی بحران‌های آینده.

۲. **مدل‌های پیش‌بینی:** طراحی و بهبود مدل‌های پیش‌بینی بحران بر اساس داده‌های تاریخی و عوامل تأثیرگذار، با استفاده از تکنیک‌های یادگیری ماشینی.

۳. **شبکه‌های عصبی عمیق:** تحقیق در مورد کاربرد شبکه‌های عصبی عمیق در تشخیص و پیش‌بینی بحران‌های امنیتی، مانند حملات سایبری و تهدیدات فیزیکی.

۴. **سیستم‌های خودمختار:** مطالعه در مورد سیستم‌های خودمختار مبتنی بر هوش‌مصنوعی که می‌توانند به صورت خودکار واکنش‌های اولیه به بحران‌ها را مدیریت کنند.

۵. **تحلیل احساسات عمومی:** بررسی و تحلیل داده‌های اجتماعی برای ارزیابی تأثیرات بحران‌ها بر احساسات عمومی و استفاده از این داده‌ها در برنامه‌ریزی و مدیریت بحران.

۶. **چالش‌های استفاده از هوش مصنوعی:** استفاده از هوش مصنوعی چالش‌هایی را به همراه دارد که نیاز است به آن پرداخته شود هرچند که با تحقیق و توسعه مداوم، می‌توان به راه‌حل‌هایی برای این مشکلات دست‌یافت.

منابع

مقالات

- امیری، عبدالرضا (۱۳۹۱). **مطالعه فرایند و متغیرهای مؤثر بر امنیتی‌شدن بحران‌های اجتماعی در ایران**، فصلنامه مطالعات مدیریت انتظامی، سال هفتم، شمارهٔ دوم، ۲۱۹-۲۳۷.
- حاجیانی، ابراهیم (۱۳۹۰)، **هشداردهی: کارکرد تحلیل اطلاعاتی در پیشگیری از غافلگیری**، فصلنامه مطالعات راهبردی، سال چهاردهم، شماره سوم.
- حبیبی، نیک‌بخش، هادیان، مهدی (۱۳۹۵). **الگوسازی سامانهٔ هشدار اطلاعاتی نظام ملی در بحران‌های امنیتی با استفاده از الگوی هشدار هوایی سریع**، فصلنامه فرماندهی و کنترل، سال اول، شماره ۱.
- حیدری، حسین (۱۴۰۱). **نقش برآورد اطلاعاتی در پیشگیری از بحران‌های امنیتی جمهوری اسلامی ایران**، فصلنامه پژوهش‌های اطلاعاتی - امنیتی دانشگاه جامع امام حسین (علیه‌السلام)، سال یازدهم، شماره ۴۱، بهار۱۴۰۱، صص ۷-۳۰.
- ربیعی، علی، خسروی، صدرا (۱۳۸۹). **مدیریت فرمانشی بحران‌های ارتباطی: الگوی متکی بر ترکیب هوش‌مصنوعی و جمعی**، فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، سال ششم، شماره ۲۱، زمستان ۱۳۸۹، صص ۳۳-۵۴.
- رئیسی، محمد، پیشگاه‌هادیان، حمید، ایزدی، جهانبخش، جاودانی مقدم، مهدی (۱۳۹۸). **آسیب‌شناسی بحران‌های اجتماعی و الزامات سیاست‌گذاری امنیتی در پیشگیری از آن**، نشریه امنیت ملی، دوره ۹، شماره ۳۲،۷۵-۱۰۲.
- شریفی دهسری، مریم، تاجفر، امیرهوشنگ (۱۴۰۲). **بررسی تأثیر به‌کارگیری هوش مصنوعی و پردازش تصویر در سیستم دبیرخانه (مرکزآمار ایران)**، هفتمین همایش ملی تحقیقات میان‌رشته‌ای در مدیریت و علوم انسانی، آبان ۱۴۰۲.
- صادقی‌زرینی، آمنه، گودرزی، ایمان، دهقان‌پور، ایرج، باجلان، مهدی (۱۴۰۲). **نقش هوش‌مصنوعی در آموزش، نشریه تحقیقات راهبردی در تعلیم و آموزش و پرورش**، شماره ۱۰، زمستان ۱۴۰۲، صص ۵۶۷ -۵۸۳.
- عارفی، عباس، رحمانی ساعد، هادی، محمدی، محمد، ابراهیمی، حسین (۱۴۰۲). **نقش مردم در مدیریت بحران‌های امنیتی در مرحله پیش‌بینی**، نشریه علمی مدیریت بحران در وضعیت‌های اضطراری، دانشگاه جامع امام حسین (علیه السلام)، سال چهاردهم، تابستان۱۴۰۲، صص۶۱-۸۹.
- عباسی، حجت، سیوندیان، مرضیه (۱۳۹۹). **مدیریت دانش و بررسی نقش هوش‌مصنوعی و سیستم‌های خبره در انواع آن**، فصلنامه پژوهش‌های معاصر در علوم مدیریت و حسابداری، سال دوم، شماره ۴، بهار ۱۳۹۹، صص ۶۷-۸۰.
- عبدی، آیدا (۱۳۹۶). **بررسی وضعیت فناوری هوش‌مصنوعی در ایران و جهان**، معاونت پژوهش‌های زیربنایی و امور تولیدی دفترمطالعات ارتباطات و فناوری‌های نوین، کد موضوعی: ۲۸۰، شماره مسلسل: ۱۵۴۹۳.

- فیروزی، محرمعلی، (۱۳۸۵). **ایران و تهدیدات ناشی از موقعیت جغرافیایی آن**، مجله آموزش جغرافیا، شماره ۷۴.
- محمود بابویی، محمودرضا، ذوالفقاری، حسین، رادان، احمدرضا، بیات، بهرام (۱۴۰۰). **نقش مؤلفه‌های اطلاعات و امنیت در تعامل مدیریت بحران‌های امنیتی**، فصلنامه علمی امنیت ملی، سال دوازدهم، شماره ۴۶، زمستان۱۴۰۱، مقاله پژوهشی از صفحات ۷-۳۲.
- میرنظامی، متینه السادات، برادران، زهره، (۱۴۰۱). **تبعات حقوقی و سیاسی کلان داده‌ها در صلح و امنیت بین المللی**، مجموعه مقالات سمپوزیوم -تأثیرعلم و فناوری‌های نوین بر صلح و امنیت بین المللی.
- رحیمی‌کلور، حسین، قاسمی‌همدانی، ایمان (۱۴۰۲). **واکاوی نقش مدیریت ریسک مبتنی بر هوش مصنوعی در افزایش چابکی و قابلیت‌های مهندسی مجدد زنجیره تأمین**. سیاست‌نامه علم‌وفناوری، دوره ۱۳، شماره ۳، پاییز ۱۴۰۲، صص ۵-۲۳.
- مدیریت بحران تحت کنترل فناوری‌های نوین (۱۳۹۸). وایت پیپر مدیریت بحران، گروه علمی‌تحلیل طیف.
- نجات‌پور، مجید، فرخی، مرتضی، سجادی، محسن، هادی‌پور، میثم (۱۴۰۱). **تحلیل جایگاه هوش‌مصنوعی در توسعه سازمان‌های نظامی**، فصلنامه مدیریت و پژوهش‌های دفاعی، سال بیست و یکم، شماره نود و هشتم، زمستان ۱۴۰۱، صفحات ۱۱-۳۲
- **هوش مصنوعی؛ تهدید یا فرصت برای امنیت ملی**، نشریه اندیشکده تحول دیجیتال، ماهنامه هوش‌مصنوعی، شماره ششم، مهرماه ۱۴۰۰.

کتاب‌ها

- ساوه درودی، مصطفی (۱۴۰۰)، **هندسه امنیت در مدیریت بحران (باتأکید برمحیط امنیتی ج.ا.ا)**، انتشارات دانشکده علوم و فنون فارابی، چاپ اول.
- زواری، عبدالمجید، طیبس، ابوالفضل(۱۴۰۱)، **کارکردهای هوش‌مصنوعی در سیاست خارجی**، اندیشکده صنایع نرم: اندیشکده روابط بین‌الملل، چاپ اول.

مقالات خارجی

- Butt, Umair Muneer, et al (2021). Spatio-temporal crime predictions by leveraging artificial intelligence for citizens security in smart cities, IEEE Access 9 (2021): 47516-47529.
- El Hajj, Mohammad, Hammoud, Jamil (2023). "Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations." Journal of Risk and Financial Management 16.10: 434.
- Radulov, N. (2019). Artificial intelligence and security. Security 4.0. Security & Future, 3(1), 3-5.

- Sun, W., Bocchini, P., & Davison, B. D. (2020). Applications of artificial intelligence for disaster management. Natural Hazards, 103(3), 2631-2689.