



هوش مصنوعی در امنیت عمومی

محمد بهرامی^۱، هاشم ثابت سیار^۲

چکیده

هدف اصلی این پژوهش، بررسی و تحلیل تأثیر فناوری هوش مصنوعی بر امنیت عمومی است. این تحقیق به دنبال پاسخ به این سوال است که چگونه فناوری هوش مصنوعی می‌تواند به بهبود امنیت عمومی کمک کند. در همین راستا، سه جلسه گروه کانونی آنلاین با متخصصان حوزه هوش مصنوعی و آشنا به مباحث امنیت عمومی برگزار شد. در این جلسات، سوال پژوهش به مباحثه گذاشته شد و دیدگاه‌های مختلف متخصصان در خصوص کاربردهای هوش مصنوعی در امنیت عمومی گردآوری و جمع‌بندی گردید. یافته‌ها نشان می‌دهد، هوش مصنوعی به عنوان یکی از پیشرفته‌ترین فناوری‌های عصر حاضر، می‌تواند نقش بسیار مهمی در بهبود امنیت عمومی ایفا کند. این فناوری، با استفاده از قابلیت‌های گسترده خود، به طور چشمگیری از شش طریق تصمیم‌گیری دقیق‌تر و سریع‌تر، نظارت و پایش بهتر، مدیریت بحران فعال، هماهنگی ارتباطی مؤثرتر، تخصیص بهتر منابع و خودکارسازی فرآیندها به تحقق امنیت عمومی کمک می‌کند.

واژگان کلیدی: هوش مصنوعی، فناوری‌های دیجیتال، امنیت، امنیت عمومی

۱. دانش آموخته دانشگاه تهران ۱. (نویسنده مسئول) Mohamad.bahrami@ut.ac.ir

۲. دانشجوی روابط بین‌الملل دانشگاه تهران. sabetsayarhashem@gmail.com



مقدمه و بیان مسئله

هوش مصنوعی^۱ به سرعت در حال تحول حوزه‌های مختلف، به ویژه سیاست‌گذاری عمومی است. این فناوری با تحلیل داده‌ها به شناسایی و اولویت‌بندی مسائل جامعه کمک می‌کند و سیاست‌هایی مبتنی بر شواهد را ممکن می‌سازد (بابائیان و همکاران، ۱۴۰۲). طبق پیش‌بینی‌ها، هوش مصنوعی که فناوری تقلید از توانایی مغز انسان در یادگیری، تحلیل و تصمیم‌گیری می‌باشد (میکالف و گوپتا^۲، ۲۰۲۱) به زودی بسیاری از جنبه‌های زندگی بشر را دگرگون خواهد کرد. کشورها نیز از این فناوری برای تقویت امنیت و قدرت خود بهره خواهند برد (نمکی و همکاران، ۱۴۰۲). فناوری‌های هوش مصنوعی به سرعت در حال گسترش ظرفیت‌های دولت‌ها هستند و نقش آن‌ها در حکمرانی، مدیریت و عملیات اجرایی به شکل چشمگیری افزایش یافته است. استفاده از این فناوری‌ها به یک ضرورت اجتناب‌ناپذیر در عصر حاضر تبدیل شده و در آینده‌ای نزدیک، نه تنها به اصلی‌ترین ابزار اداره کشور تبدیل خواهد شد (دانایی فرد، ۱۴۰۱)، بلکه به حکمرانی مؤثرتر کمک خواهد نمود (آرودا^۳ و همکاران، ۲۰۲۴). انتظار می‌رود نقش هوش مصنوعی به صورت روزافزون در تضمین امنیت عمومی رشد داشته باشد (ماهور^۴ و همکاران، ۲۰۲۳). این فناوری با بهبود سیستم‌های پشتیبانی تصمیم‌گیری و بهینه‌سازی عملیات به یکی از ابزارهای کلیدی در تضمین امنیت عمومی کشورها تبدیل شده است (وامبا^۵، ۲۰۱۹).

با عنایت به این موضوع که هوش مصنوعی به یکی از فناوری‌های کلیدی در تغییر و تحول عرصه‌های مختلف زندگی بشر تبدیل شده است و به ویژه در زمینه امنیت عمومی، به علت توانایی‌های بالای خود در تحلیل داده‌ها و بهینه‌سازی فرآیندها، نقش مهمی ایفا می‌کند، بررسی دقیق تأثیرات این فناوری بر امنیت عمومی و نحوه بهره‌برداری مؤثر از آن در راستای بهبود امنیت کشور، مسئله‌ای اساسی و ضروری است. در همین راستا، هدف اصلی این تحقیق بررسی و تحلیل نقش هوش مصنوعی در ارتقاء و بهبود امنیت عمومی است. به عبارتی، این مطالعه به دنبال پاسخ به این سوال است که:

چگونه فناوری هوش مصنوعی می‌تواند به بهبود امنیت عمومی کمک نماید؟

1. Artificial intelligence
2. Mikalef & Gupta
3. Arruda
4. Mahor
5. Wamba



بنابراین، این تحقیق به دنبال شناسایی و بررسی کاربردهای مختلف فناوری هوش مصنوعی در تقویت سیستم‌های امنیتی، بهینه‌سازی فرآیندهای تصمیم‌گیری و افزایش کارایی عملیات امنیتی است. ضرورت تحقیق در این است که بررسی تأثیرات این فناوری بر امنیت عمومی می‌تواند به بهبود روش‌های مقابله با تهدیدات و ارتقاء کارایی سیستم‌های امنیتی کمک کند. این تحقیق همچنین به شناسایی چالش‌ها و فرصت‌های بهره‌برداری مؤثر از هوش مصنوعی در حوزه امنیت عمومی پرداخته و به توسعه راهکارهای مناسب برای این منظور یاری می‌رساند.

در انجام تحقیق، ابتدا به بررسی مطالعات پیشین پرداخته شد و مطالعاتی که به‌طور مستقیم به موضوع مرتبط بودند، تشریح شدند. سپس، از طریق برگزاری سه جلسه گروه کانونی برخط^۱ با متخصصان حوزه، سوال پژوهشی به بحث و بررسی گذاشته شد. در نهایت، با تقاطع‌گیری مطالب نظری و نتایج و یافته‌های جلسات مباحثه، چندین روش اصلی که از آن طریق هوش مصنوعی در امنیت عمومی نقش‌آفرینی می‌کند، شناسایی گردید.

امید است این تحقیق به توسعه نظریه‌ها و مدل‌های علمی در زمینه کاربرد هوش مصنوعی در امنیت عمومی و به غنی‌سازی ادبیات علمی در این حوزه کمک کند. همچنین، شناسایی روش‌های اصلی نقش‌آفرینی هوش مصنوعی در امنیت عمومی به بهبود ارتقای راهبردهای امنیتی و کارایی سیستم‌های امنیتی کمک می‌کند.

پیشینه نظری

امنیت

امنیت به وضعیت یا شرایطی اطلاق می‌شود که در آن افراد، جوامع، سازمان‌ها و کشورها از تهدیدات و خطرات مختلف محافظت می‌شوند. این مفهوم به معنای فقدان تهدید نیست، بلکه به معنای توانایی مدیریت و کاهش تهدیدات به گونه‌ای است که تأثیرات منفی آن‌ها به حداقل برسد. امنیت می‌تواند شامل محافظت از جان، مال، اطلاعات، و ارزش‌های فرهنگی و اجتماعی باشد. در واقع، امنیت به معنای ایجاد یک محیط امن و پایدار است که در آن افراد و جوامع می‌توانند به فعالیت‌های روزمره خود بپردازند بدون اینکه نگران تهدیدات و خطرات مختلف باشند (بالدوین^۲، ۱۹۹۷). امنیت به دو شاخه امنیت داخلی و امنیت خارجی تقسیم می‌شود.

1. Online Focus group
2. Baldwin



امنیت داخلی ناظر بر حفظ نظم و قانون در داخل کشور است و شامل اقداماتی از قبیل جلوگیری از جرم و جنایت، مدیریت بحران‌های داخلی، بلایای طبیعی و حفظ نظم عمومی می‌باشند. امنیت خارجی نیز به مجموعه‌ای از اقدامات و سیاست‌هایی اطلاق می‌شود که به منظور محافظت از کشور در برابر تهدیدات خارجی مانند حملات نظامی، تروریسم بین‌المللی، و تجاوزات خارجی انجام می‌شود (والث،^۱، ۱۹۹۱).

امنیت عمومی

امنیت عمومی به مجموعه‌ای از اقدامات و سیاست‌هایی گفته می‌شود که به منظور حفظ و ارتقاء امنیت و سلامت شهروندان در جامعه انجام می‌شود. این مفهوم به عنوان بخشی از امنیت ملی مورد توجه قرار دارد و شامل محافظت از افراد در برابر تهدیدات مختلفی مانند جنایت، تروریسم، بلایای طبیعی، و حوادث صنعتی است (ریس،^۲، ۲۰۱۲؛ کلینگ و کولز،^۳، ۱۹۹۶). مفهوم امنیت عمومی را می‌توان در چهار حوزه اصلی امنیت فیزیکی، امنیت سایبری، امنیت بهداشتی و امنیت اجتماعی مورد بررسی قرار داد (ریس، ۲۰۱۲؛ کلینگ و کولز، ۱۹۹۶). امنیت فیزیکی، شامل اقداماتی است که برای محافظت از افراد و اموال در برابر تهدیدات فیزیکی مانند سرقت، حملات تروریستی، و حوادث طبیعی انجام می‌شود. این اقدامات می‌توانند شامل نصب دوربین‌های مدار بسته، استفاده از نگهبانان، و ایجاد سیستم‌های هشدار دهنده باشند (سینها^۴ و همکاران، ۲۰۱۵). امنیت سایبری، به محافظت از اطلاعات و سیستم‌های دیجیتال در برابر تهدیدات سایبری مانند هک، بدافزارها، و حملات فیشینگ اشاره دارد. این حوزه شامل استفاده از فایروال‌ها، نرم‌افزارهای ضد ویروس، و پروتکل‌های امنیتی مختلف است (سینها و همکاران، ۲۰۱۵). امنیت بهداشتی، شامل اقداماتی است که برای حفظ سلامت عمومی و جلوگیری از انتشار بیماری‌ها انجام می‌شود. این اقدامات می‌توانند شامل واکسیناسیون، کنترل بیماری‌های واگیر، و مدیریت بحران‌های بهداشتی مانند پاندمی‌ها باشند (آلدیس،^۵، ۲۰۰۸). و در نهایت، امنیت اجتماعی، به ایجاد و حفظ محیطی امن و پایدار برای زندگی اجتماعی اشاره دارد. این حوزه شامل جلوگیری از جرم و جنایت، ارتقاء عدالت

1. Walt
2. Reese
3. Kelling & Cole
4. Sinha
5. Aldis



اجتماعی، و فراهم کردن خدمات اجتماعی مانند آموزش و بهداشت است (گونزالس-ایراس و نیپلت^۱، ۲۰۰۸).

امنیت عمومی به عنوان یکی از مهم‌ترین مسئولیت‌های حکومت‌ها محسوب می‌شود. ایجاد و حفظ محیطی امن و پایدار برای زندگی شهروندان نه تنها به رفاه و آسایش آنان کمک می‌کند، بلکه زمینه را برای توسعه اقتصادی، اجتماعی و فرهنگی جامعه نیز فراهم می‌سازد. به همین دلیل، تقویت امنیت عمومی به عنوان یک اولویت راهبردی در دستور کار بسیاری از کشورها قرار دارد. دولت‌ها همواره با تهدیدات مختلفی در حوزه امنیت عمومی مانند سیستم‌های قانونی ناکارآمد، نارضایتی‌های اجتماعی و اقتصادی، نقصان در آموزش و نهادهای اجتماعی، تغییرات جمعیتی و مشکلات زیرساختی و... مواجه هستند (هیدوک^۲، ۲۰۲۰). برای مقابله با این تهدیدها، فناوری‌های جدید مانند هوش مصنوعی نقش بسیار مهمی در بهبود کیفیت و کارایی عملیات مدیریتی و اجرایی دارند که این امر می‌تواند تأثیرات مثبتی برای کشور به همراه داشته باشد.

هوش مصنوعی

نخستین ایده‌های مربوط به هوش مصنوعی به دوران باستان بازمی‌گردد، اما پیشرفت‌های واقعی در این زمینه با توسعه رایانه‌ها در قرن بیستم آغاز شد. آلن تورینگ، یکی از پیشگامان علوم رایانه، در دهه ۱۹۵۰ با ارائه تست تورینگ، مفهومی که بیان می‌کرد اگر یک ماشین بتواند یک مکالمه انسانی را به طوری تقلید کند که فرد مقابل نتواند تفاوتی بین ماشین و انسان تشخیص دهد، می‌توان آن ماشین را "هوشمند" دانست، نقش مهمی در شکل‌گیری ایده‌های مدرن هوش مصنوعی ایفا کرد. دهه‌های ۱۹۵۰ و ۱۹۶۰ شاهد اولین تلاش‌ها برای ساخت سیستم‌های هوش مصنوعی بود. جان مک‌کارتی و ماروین مینسکی از پیشگامان اصلی این حوزه بودند. مک‌کارتی در سال ۱۹۵۶ در کنفرانسی در دانشگاه دارتموث، اصطلاح "هوش مصنوعی" را ابداع کرد و هدف اولیه آن ساخت ماشین‌های هوشمندی بود که قادر به انجام وظایف شناختی انسان بودند (زونیکا^۳، ۲۰۲۳).

هوش مصنوعی، فناوری تقلید از توانایی مغز انسان در یادگیری، تحلیل و تصمیم‌گیری

1. Gonzalez-Eiras & Niepelt
2. Hejduk
3. Zúñiga



می‌باشد (میکالف و گوپتا، ۲۰۲۱). به عبارت دیگر هوش مصنوعی به توانایی ماشین‌ها و سیستم‌های کامپیوتری برای انجام وظایفی اطلاق می‌شود که معمولاً نیازمند هوشمندی انسانی است. این توانایی شامل یادگیری، استدلال، تشخیص الگو، تصمیم‌گیری و حل مسئله است. هوش مصنوعی با استفاده از الگوریتم‌ها و داده‌های گسترده، قادر است رفتار و واکنش‌های انسان‌ها را تحلیل و پیش‌بینی کند (نمکی و همکاران، ۱۴۰۲). هوش مصنوعی به دو دسته اصلی تقسیم می‌شود: هوش مصنوعی ضعیف^۱ که برای انجام یک وظیفه خاص طراحی شده است و هوش مصنوعی قوی^۲ که هدف آن دستیابی به هوش عمومی نزدیک به هوش انسان است. تکنیک‌های ساخت هوش مصنوعی نیز به‌طور کلی در دو گروه روش یادگیری ماشین^۳ و یادگیری عمیق^۴ بررسی می‌شوند. یادگیری ماشین تکنیکی است که در آن الگوریتم‌ها از داده‌ها یاد می‌گیرند و با تجزیه و تحلیل الگوها عمل می‌کنند. یادگیری عمیق زیرشاخه‌ای از یادگیری ماشین است که از شبکه‌های عصبی عمیق برای پردازش داده‌ها استفاده می‌کند. این شبکه‌ها از مجموعه‌ای از لایه‌های به هم پیوسته تشکیل شده‌اند که هر لایه آنالیز پیچیده‌تر و عمیق‌تری از داده‌ها ارائه می‌دهد (زونینگ و همکاران، ۲۰۲۳).

سیستم‌های هوش مصنوعی هم‌اکنون در صنایع متعددی از جمله بهداشت و درمان، حمل و نقل، مالی و حتی حقوقی به کار گرفته می‌شوند. این سیستم‌ها قادر به انجام وظایفی هستند که به نظر می‌رسید تنها توسط انسان‌ها قابل انجام باشد، نظیر تشخیص بیماری، تحلیل بازارهای مالی و رسیدگی به مسائل حقوقی. علاوه بر پیشرفت‌های فنی، مسئله اخلاق در هوش مصنوعی به یکی از داغ‌ترین موضوعات روز تبدیل شده است. ایجاد سیستم‌هایی که قابلیت‌هایی نزدیک به هوش انسان داشته باشند، سوالات جدی در خصوص اخلاقی بودن استفاده از این سیستم‌ها، مسئولیت‌پذیری، و تأثیرات اجتماعی-اقتصادی آن‌ها ایجاد کرده است. پژوهشگران و سیاست‌گذاران در سراسر جهان در تلاش هستند تا چارچوب‌های قانونی و اخلاقی مناسبی برای تنظیم استفاده از هوش مصنوعی ایجاد کنند (هانلین و کاپلان، ۲۰۱۹).

1. Narrow AI
2. Strong AI
3. Machine Learning
4. Deep Learning
5. Haenlein & Kaplan



هوش مصنوعی و امنیت عمومی

نینگ^۱ (۲۰۲۴). در مقاله خود هوش مصنوعی را به عنوان تکنولوژی دیجیتال و تکنولوژی هوشمند و به عنوان ابزاری در مدیریت عمومی تعریف می‌کند. تکنولوژی دیجیتال به دیجیتالی شدن امور مختلف در مدیریت عمومی و جمع‌آوری حجم عظیمی از امور عمومی اشاره دارد. تکنولوژی هوشمند نیز به عنوان ابزاری برای بهبود کارایی مدیریت اجتماعی و عمومی، افزایش ماهیت علمی تصمیم‌گیری اداری، بهینه‌سازی فرآیند مدیریت اداری، کاهش زمان و هزینه‌های اقتصادی مدیریت عمومی، هشدار اولیه در مورد بحران‌های عمومی و کاهش خسارات مدیریت بحران مورد استفاده قرار می‌گیرد. نویسنده به کاربرد گسترده فناوری شناسایی چهره در مدیریت امنیت عمومی اشاره می‌کند. این سیستم شناسایی چهره در مناطق مسکونی، تجاری و حمل و نقل عمومی استفاده می‌شود و قادر به شناسایی و ردیابی افراد خاص و مسیرهای آن‌ها است. این سیستم می‌تواند به طور خودکار هشدار دهد و به حل پرونده‌ها کمک کند. و در نهایت، لزوم وضع قوانین و محدودیت‌ها برای استفاده از فناوری‌های هوش مصنوعی در مدیریت امنیت عمومی را مورد تأکید قرار می‌دهد.

دانائی فرد (۱۴۰۲). در مطالعه خود به بررسی نحوه استفاده از تکنولوژی‌های هوش مصنوعی در فرآیند حکمرانی می‌پردازد و استدلال می‌کند که هوش مصنوعی می‌تواند به دولت‌ها کمک کند تا تخصیص منابع عمومی را از طریق تحلیل داده‌ها و شناسایی الگوها بهینه‌سازی کنند. همچنین هوش مصنوعی می‌تواند با فراهم کردن تحلیل داده‌های سریع و دقیق، از تصمیم‌گیری مبتنی بر شواهد و سیاست‌گذاری حمایت کند و ارتباط و هماهنگی بین دولت، شهروندان و سایر ذینفعان را بهبود بخشد. استفاده صحیح از هوش مصنوعی می‌تواند ضمن تسهیل دسترسی به داده‌ها و اطلاعات جامع، خطاهای انسانی در فرآیندهای حکمرانی را کاهش دهد. نویسنده هوش مصنوعی را به عنوان یک تکنولوژی تعریف می‌کند که می‌تواند تحلیل داده‌ها را سریع‌تر و دقیق‌تر انجام دهد تا از تصمیم‌گیری مبتنی بر شواهد در حکمرانی حمایت کند. همچنین ارتباط و هماهنگی بین دولت و شهروندان/ذینفعان را بهبود بخشد و خطاهای انسانی در فرآیندهای حکمرانی را از طریق دسترسی به داده‌ها و اطلاعات جامع کاهش دهد. بر این اساس ارتباط هوش مصنوعی با امنیت عمومی را در می‌توان در مواردی از قبیل بهینه‌سازی منابع، سیاست‌گذاری مبتنی بر شواهد، بهبود ارتباطات و همچنین کاهش خطاهای انسانی، با این توضیح تعریف نمود که:

1. Ning



۱. هوش مصنوعی می‌تواند به دولت‌ها کمک کند تا تخصیص منابع عمومی را از طریق شناسایی الگوها و روندها در داده‌ها بهینه‌سازی کنند. این بهینه‌سازی می‌تواند به بهبود امنیت عمومی از طریق تخصیص بهتر منابع به مناطق و بخش‌های نیازمند کمک کند.

۲. تحلیل داده‌های مبتنی بر هوش مصنوعی می‌تواند از تصمیم‌گیری‌های دقیق‌تر و مبتنی بر داده‌ها توسط سیاست‌گذاران حمایت کند. این امر می‌تواند به تدوین سیاست‌های امنیتی کارآمدتر و موثرتر منجر شود.

۳. هوش مصنوعی می‌تواند ارتباط و هماهنگی بین دولت، شهروندان و سایر ذینفعان را بهبود بخشد. بهبود ارتباطات می‌تواند به پاسخگویی سریع‌تر و موثرتر در مواقع بحران و افزایش امنیت عمومی کمک کند. و در نهایت، هوش مصنوعی می‌تواند با ارائه دسترسی به داده‌ها و اطلاعات جامع، خطاهای انسانی در فرآیندهای حکمرانی را کاهش دهد. کاهش این خطاها می‌تواند به بهبود عملکرد سیستم‌های امنیتی و کاهش خطرات مرتبط با امنیت عمومی منجر شود.

بابایان و همکاران (۱۴۰۲). به بررسی نقش هوش مصنوعی در چرخه سیاست‌گذاری عمومی از طریق رویکرد فراترکیب می‌پردازند. چرخه سیاست‌گذاری عمومی شامل چندین مرحله از جمله تعیین دستور کار، تدوین سیاست، تصمیم‌گیری، اجرای سیاست و ارزیابی سیاست است. این مطالعه به بررسی ادبیات موجود در مورد کاربرد هوش مصنوعی در هر مرحله از چرخه سیاست‌گذاری پرداخته است. نتایج نشان می‌دهد که هوش مصنوعی می‌تواند نقش مهمی در افزایش کارایی و اثربخشی چرخه سیاست‌گذاری ایفا کند، به ویژه در زمینه‌هایی مانند تحلیل داده‌ها، تصمیم‌گیری و اجرای سیاست‌ها. با این حال، این مطالعه همچنین به چالش‌ها و ملاحظات اخلاقی مرتبط با استفاده از هوش مصنوعی در بخش عمومی مانند شفافیت، پاسخگویی و تعصب اشاره می‌کند. نویسندگان استدلال می‌کنند کاربرد هوش مصنوعی در چرخه سیاست‌گذاری عمومی می‌تواند تأثیرات مهمی بر امنیت عمومی داشته باشد. سه موضوع تحلیل داده‌ها، تصمیم‌گیری و اجرای سیاست موضوعاتی است که در این مطالعه مورد تمرکز قرار می‌گیرد. هوش مصنوعی می‌تواند برای تحلیل حجم زیادی از داده‌ها از منابع مختلف از جمله سازمان‌های اجرای قانون و ایمنی عمومی استفاده شود تا الگوها، روندها و تهدیدات احتمالی شناسایی شود که می‌تواند تصمیمات سیاستی و تخصیص منابع مرتبط با امنیت عمومی را اطلاع‌رسانی کند. از سوی دیگر، سیستم‌های مبتنی بر هوش مصنوعی می‌توانند به سیاست‌گذاران و مقامات عمومی



در اتخاذ تصمیمات مبتنی بر داده‌ها و آگاهانه‌تر در مورد سیاست‌ها و مداخلات مرتبط با ایمنی و امنیت عمومی کمک کنند و در نهایت، هوش مصنوعی می‌تواند برای خودکارسازی و ساده‌سازی اجرای سیاست‌های امنیت عمومی استفاده شود، مانند استفاده از سیستم‌های نظارتی هوشمند، الگوریتم‌های پیش‌بینی جرم و فرآیندهای تصمیم‌گیری خودکار.

احمدی و همکاران (۱۴۰۲). در مقاله خود، چگونگی بکارگیری هوش مصنوعی و مزایای آن در بهبود امنیت عمومی را از هفت منظر تشریح می‌کنند.

۱. ارتقای سیستم‌های نظارتی و پیشگیری از جرم، با این توضیح که هوش مصنوعی می‌تواند با تحلیل داده‌های حجیم از دوربین‌های مداربسته و سنسورهای هوشمند، الگوهای رفتاری مشکوک را شناسایی کند. این قابلیت به نیروهای امنیتی اجازه می‌دهد تا به صورت پیشگیرانه عمل کنند و قبل از وقوع جرم یا تهدید امنیتی، اقدامات لازم را انجام دهند. سیستم‌های مبتنی بر هوش مصنوعی قادرند با دقت بالا و در زمان واقعی، تصاویر و ویدئوها را پردازش کرده و موارد مشکوک را به سرعت به مسئولین مربوطه گزارش دهند.

۲. بهبود مدیریت بحران و واکنش سریع، به این ترتیب که، در زمان وقوع بحران‌های امنیتی، هوش مصنوعی می‌تواند با تحلیل سریع اطلاعات از منابع مختلف، به تصمیم‌گیری بهتر و سریع‌تر کمک کند. الگوریتم‌های پیشرفته قادرند سناریوهای مختلف را شبیه‌سازی کرده و بهترین روش‌های مقابله با بحران را پیشنهاد دهند. همچنین، سیستم‌های هوش مصنوعی می‌توانند در هماهنگی نیروها و منابع در زمان بحران نقش مهمی ایفا کنند و باعث افزایش کارایی و اثربخشی عملیات‌های لازم شوند.

۳. پیش‌بینی و شناسایی تهدیدات سایبری، با این توضیح که، با توجه به افزایش تهدیدات سایبری، هوش مصنوعی نقش حیاتی در حفاظت از زیرساخت‌های حیاتی و اطلاعات حساس دولتی ایفا می‌کند. سیستم‌های مبتنی بر هوش مصنوعی قادرند الگوهای حملات سایبری را شناسایی کرده و حتی قبل از وقوع حمله، اقدامات پیشگیرانه انجام دهند. این سیستم‌ها می‌توانند به طور مداوم شبکه‌ها را مانیتور کرده و هرگونه فعالیت مشکوک را شناسایی و مسدود کنند، که این امر به طور قابل توجهی امنیت سایبری را افزایش می‌دهد.

۴. تحلیل و پردازش اطلاعات، یعنی هوش مصنوعی می‌تواند حجم عظیمی از داده‌های خبری را در زمانی کوتاه تحلیل کند و الگوها و ارتباطات پنهان را کشف نماید. این قابلیت به سازمان‌های امنیتی کمک می‌کند تا تهدیدات را سریع‌تر شناسایی کرده و اقدامات لازم را



انجام دهند. همچنین، الگوریتم‌های یادگیری ماشین می‌توانند در تحلیل متون، صدا و تصاویر برای استخراج اطلاعات مفید، بسیار مؤثر باشند.

۵. بهبود کنترل مرزی و مدیریت مهاجرت، با این توضیح که، سیستم‌های هوش مصنوعی می‌توانند در بهبود امنیت مرزها و مدیریت مهاجرت نقش مهمی ایفا کنند. فناوری‌های تشخیص چهره و بیومتریک مبتنی بر هوش مصنوعی می‌توانند به سرعت و با دقت بالا هویت افراد را تأیید کنند. این سیستم‌ها همچنین قادرند الگوهای مشکوک در عبور و مرور مرزی را شناسایی کرده و به مقامات مربوطه هشدار دهند. علاوه بر این، هوش مصنوعی می‌تواند در پردازش سریع تر درخواست‌های مهاجرتی و شناسایی موارد مشکوک کمک شایانی کند. ۶. ارتقای سیستم‌های شناسایی و ردیابی، به ترتیبی که، هوش مصنوعی می‌تواند سیستم‌های شناسایی و ردیابی را به طور قابل توجهی بهبود بخشد. الگوریتم‌های پیشرفته قادرند افراد مظنون را در میان جمعیت شناسایی کرده و حرکات آنها را ردیابی کنند. این قابلیت در مکان‌های شلوغ مانند فرودگاه‌ها، ایستگاه‌های قطار و مراکز خرید بسیار ارزشمند است. همچنین، هوش مصنوعی می‌تواند در ردیابی وسایل نقلیه مشکوک و شناسایی الگوهای حرکتی غیرعادی کمک کند.

۷. بهبود آموزش و شبیه‌سازی سناریوهای واقعی برای نیروهای امنیتی، با این توضیح که هوش مصنوعی می‌تواند در ایجاد سناریوهای آموزشی پیشرفته و واقع‌گرایانه برای نیروهای امنیتی نقش مهمی ایفا کند. سیستم‌های شبیه‌سازی مبتنی بر هوش مصنوعی قادرند شرایط مختلف را با جزئیات دقیق شبیه‌سازی کرده و به نیروها اجازه دهند تا در محیطی امن، مهارت‌های خود را ارتقا دهند. این سیستم‌ها می‌توانند بر اساس عملکرد فرد، سناریوها را تطبیق داده و بازخورد شخصی‌سازی شده ارائه دهند، که این امر باعث افزایش کارایی آموزش و آمادگی بهتر نیروها برای مواجهه با چالش‌های واقعی می‌شود.

نمکی و همکاران (۱۴۰۲). نیز، در مقاله خود این سوال اصلی مهم را مطرح می‌کنند که تاثیر هوش مصنوعی در فرماندهی، کنترل و هدایت نبردهای ترکیبی آینده تا چه حد خواهد بود. نویسندگان به بررسی سطح آشنایی شهروندان ایرانی با هوش مصنوعی، مطالعات آینده اقدامات دشمنان و ضرورت استفاده از هوش مصنوعی برای امنیت پایدار کشور می‌پردازند؛ و بر اهمیت حضور فعال هوش مصنوعی در تحولات اخیر، به ویژه در ناآرامی‌ها و تاثیر بر نسل جوان تأکید می‌کنند و ضرورت تشکیل و تقویت شبکه اطلاعات ملی، اهمیت آموزش در امنیت ملی و هوش



مصنوعی و محدودیت استفاده از فناوری هوش مصنوعی داخلی بین مقامات عالی‌رتبه را مطرح می‌کند. هوش مصنوعی می‌تواند نقش مهمی در فرماندهی، کنترل و تصمیم‌گیری در نبردهای آینده ایفا کند. با مدیریت و کنترل صحیح، هوش مصنوعی می‌تواند به بهبود امنیت پایدار کشور از طریق راهکارهای از قبیل افزایش (۱) آگاهی موقعیتی در زمان واقعی، (۲) تحلیل دقیق، (۳) پیش‌بینی آینده نبردها و (۴) بهینه‌سازی برنامه‌های عملیاتی کمک نماید. این مطالعه بر ضرورت استفاده از هوش مصنوعی برای مقابله با اقدامات و راهبردهای آینده دشمنان علیه امنیت کشور تأکید می‌کند. به علاوه، ترکیب هوش مصنوعی با اخبار جعلی می‌تواند موجب بی‌اعتمادی مردم به اخبار و در نتیجه اختلال در اداره جامعه شود. بنابراین، مقابله با این تهدیدات نیازمند توجه جدی به حکمرانی داده و هوش مصنوعی در حوزه امنیت ملی است.

اسلایر^۱ (۲۰۲۰). در یک گزارش تحلیلی یک نمای کلی از وضعیت فعلی توسعه هوش مصنوعی و تأثیرات آن بر امنیت ملی ایالات متحده ارائه می‌دهد. این گزارش همچنین برخی از روش‌هایی که وزارت دفاع آمریکا به دنبال استفاده از هوش مصنوعی برای اطلاعات، نظارت، شناسایی، لجستیک، عملیات سایبری و سایر مأموریت‌های امنیت ملی آمریکا است را بررسی می‌کند. بر اساس این گزارش می‌توان استدلال نمود که بسیاری از کاربردهای هوش مصنوعی که برای استفاده نظامی توسعه یافته‌اند، مانند اطلاعات، نظارت و امنیت سایبری، می‌توانند در امنیت عمومی و اجرای قانون نیز مورد استفاده قرار گیرند. به عنوان مثال، تحلیل ویدیویی با هوش مصنوعی و تشخیص ناهنجاری‌ها می‌تواند آگاهی موقعیتی و قابلیت‌های پاسخگویی را بهبود بخشد. هر چند گزارش به نگرانی‌هایی درباره سوءاستفاده از فناوری‌های هوش مصنوعی مانند «دیپ فیک» برای عملیات اطلاعاتی اشاره می‌کند که می‌تواند اعتماد عمومی را تضعیف کند. این نوع کمپین‌های اطلاعات نادرست با هوش مصنوعی می‌تواند خطراتی برای امنیت عمومی ایجاد کند و باعث سردرگمی و کاهش اعتماد به دولت و نهادها شود.

بر اساس مطالعات کلی و همکاران^۲ (۲۰۲۳). یکی از مهم‌ترین عواملی که در پذیرش هوش مصنوعی تأثیرگذار است، سودمندی ادراک‌شده است. این عامل بیانگر این است که کاربران تا چه اندازه اعتقاد دارند که استفاده از یک سیستم هوش مصنوعی می‌تواند کارایی و عملکرد آن‌ها را بهبود بخشد. مطالعات متعددی نشان داده‌اند که زمانی که کاربران باور دارند یک سیستم هوش

1. Slayer
2. Kelly et al



مصنوعی می‌تواند به نیازهای آن‌ها پاسخ دهد و در انجام وظایف آن‌ها مفید باشد، احتمال استفاده آن‌ها از این فناوری بیش‌تر خواهد بود. علاوه بر سودمندی، انتظار عملکرد نیز عامل مهم دیگری است که نقش بسزایی در پذیرش هوش مصنوعی دارد. در مقابل، عواملی مانند نیاز به تماس انسانی و حضور فیزیکی می‌توانند مانع پذیرش هوش مصنوعی شوند. در برخی از فرهنگ‌ها و صنایع، تعاملات انسانی نقش مهمی در انجام وظایف دارند و تلاش برای جایگزینی این تعاملات با سیستم‌های هوش مصنوعی ممکن است با مقاومت مواجه شود. بنابراین برای موفقیت در پذیرش و ادغام هوش مصنوعی در این جوامع و صنایع، نیاز است که فرآیندهای موجود به‌صورت هوشمندانه‌ای طراحی و پیاده‌سازی شوند که هم توانایی‌های هوش مصنوعی را به کار گیرد و هم ضرورت‌های انسانی را مورد توجه قرار دهد.

پولتو^۱ و همکاران (۲۰۲۳). به تحلیل و جبهه‌های تحقیقاتی در زمینه کاربردهای امنیت اطلاعات در شهرهای هوشمند می‌پردازند تا مرزهای تحقیقاتی، روندها و فرصت‌های جدید در این حوزه را شناسایی کنند. نویسندگان از تحلیل‌های بیبلیومتریک برای شناسایی محققان تاثیرگذار و آثار آنها بر تحقیقات با موضوع امنیت اطلاعات و شهرهای هوشمند استفاده کرده‌اند. بر این اساس استدلال می‌شود که فناوری‌های هوش مصنوعی می‌توانند برای بهبود جنبه‌های مختلف امنیت و ایمنی در شهرهای هوشمند به کار گرفته شوند که مثال‌هایی از این کاربردها عبارتند از: نظارت و پایش، پلیس پیش‌بینی‌کننده، امنیت سایبری، پاسخ به وضعیت‌های اضطراری و مدیریت زیرساخت‌های عمومی. هوش مصنوعی در زمینه پلیس پیش‌بینی‌کننده می‌تواند انقلابی در روش‌های فعلی پلیسی ایجاد کند. مدل‌های پیش‌بینی مبتنی بر هوش مصنوعی می‌توانند داده‌های تاریخی مرتبط با جرم و جنایت را تحلیل کرده و الگوهای جرم را شناسایی کنند. این مدل‌ها می‌توانند نقاط حساس و کلیدی مرتبط با جرائم را پیش‌بینی کنند و اطلاعات لازم را به نیروهای پلیس ارائه دهند تا اقدامات پیشگیرانه انجام گیرد. یکی از تکنیک‌های اصلی در این زمینه، یادگیری ماشین است که از داده‌های گذشته برای پیش‌بینی حوادث آینده استفاده می‌کند. الگوریتم‌های یادگیری عمیق می‌توانند از دامنه وسیعی از متغیرها استفاده کنند، شامل داده‌های دموگرافیک، الگوهای تردد، و موضوعات اقتصادی مرتبط. پلیس می‌تواند از این پیش‌بینی‌ها برای تعیین محل‌های حساس و مهم استفاده کند. نتایج مثبت پلیس پیش‌بینی‌کننده شامل کاهش وقوع جرم، بهبود اعتماد عمومی به نیروهای امنیتی، و استفاده بهینه از منابع پلیسی است.



لاولی و همکاران^۱ (۲۰۲۳). در مطالعه خود به بررسی وضعیت فعلی تحقیقات مرتبط با استفاده از هوش مصنوعی در خدمات عمومی می‌پردازند که در پایگاه داده اسکوپوس^۲ نمایه شده‌اند. علاوه بر این، تحلیل نتایج جستجو در پایگاه داده اسکوپوس، ویژگی‌ها و روندهای مجلات، نویسندگان و موضوعات مرتبط با کاربرد هوش مصنوعی در تحقیقات خدمات عمومی را به تصویر می‌کشد. بر اساس نتایج این مطالعه، هوش مصنوعی می‌تواند به هوشمندتر شدن شهرها کمک کند و با بهبود کیفیت زندگی شهروندان و افزایش کارایی دسترسی آن‌ها به کالاها و خدمات عمومی، نقش آفرینی کند. با طراحی و پیاده‌سازی راهبردی فناوری مبتنی بر هوش مصنوعی، خدمات عمومی سنتی می‌توانند به خدمات هوشمند تبدیل شوند. این مطالعه مواردی را به عنوان ظرفیت‌های قابل بهره‌برداری این فناوری‌ها پیشنهاد می‌کند، به این ترتیب که،

۱. هوش مصنوعی می‌تواند به بهبود فرآیندهای دولتی و خدمات عمومی کمک کند. این امر می‌تواند شامل بکارگیری سیستم‌های پیشرفته نظارتی، تحلیل داده‌های بزرگ برای پیش‌بینی و پیشگیری از جرائم، و بهبود پاسخ‌دهی در شرایط اضطراری باشد که همگی به طور مستقیم بر امنیت عمومی تأثیر می‌گذارند.

۲. در شرایط شغلی خطرناک، ربات‌های مجهز به هوش مصنوعی می‌توانند جایگزین انسان‌ها شوند. این امر نه تنها از آسیب‌های شغلی جلوگیری می‌کند، بلکه می‌تواند در عملیات‌های نجات و امداد خطرناک نیز مورد استفاده قرار گیرد، که به نوبه خود امنیت عمومی را افزایش می‌دهد.

۳. هوش مصنوعی می‌تواند به تسهیل حرکت به سمت عملیات دولتی پایدار کمک کند. این امر می‌تواند شامل مدیریت بهتر منابع، کاهش آلودگی و بهبود زیرساخت‌های شهری باشد که همگی به طور غیرمستقیم بر امنیت و سلامت عمومی تأثیر می‌گذارند.

۴. استفاده از هوش مصنوعی در بخش دولتی می‌تواند سیاست‌گذاری، ارائه خدمات عمومی و مدیریت داخلی را بهبود بخشد. این امر می‌تواند منجر به تصمیم‌گیری‌های بهتر در زمینه امنیت عمومی، توزیع عادلانه‌تر منابع و پاسخگویی سریع‌تر به نیازهای امنیتی جامعه شود. و در نهایت، هوش مصنوعی می‌تواند به تبدیل خدمات عمومی سنتی به خدمات هوشمند کمک کند. این امر می‌تواند شامل سیستم‌های هوشمند مدیریت ترافیک، پیش‌بینی و مدیریت بلایای طبیعی، و سیستم‌های پاسخ اضطراری پیشرفته باشد که همگی به طور مستقیم امنیت عمومی را بهبود می‌بخشند.

1. Lawelai et al

2. Scopus



بر اساس مطالب ارائه شده در مقالات بالا، نقش هوش مصنوعی در امنیت عمومی از طریق (۱) کمک به تصمیم‌گیری، (۲) ارتقای سیستم‌های نظارتی، (۳) مدیریت بحران و واکنش‌های سریع در شرایط اضطرار، (۴) ارتقای هماهنگی و ارتباطات، (۵) خودکارسازی و کاهش خطاهای انسانی مورد تمرکز و توجه قرار گرفته است. این اشتراکات نشان‌دهنده تأثیر عمده‌ای است که هوش مصنوعی می‌تواند در افزایش کارآمدی، دقت و سرعت در فرآیندهای مرتبط با امنیت عمومی داشته باشد.

روش تحقیق

روش تحقیق به مجموعه‌ای از فرآیندها و روش‌هایی گفته می‌شود که به کمک آن‌ها اطلاعات جمع‌آوری، تحلیل و تفسیر می‌شوند تا جواب سؤالات تحقیق به دست آید. روش تحقیق در واقع چگونگی دستیابی به دانش و ادبیات جدید در یک حوزه خاص می‌باشد. بطور کلی، روش‌های تحقیق به دو دسته اصلی کمی و کیفی تقسیم می‌شوند. روش‌های کمی شامل جمع‌آوری و تحلیل داده‌های عددی هستند و از آمار و ریاضیات برای تحلیل استفاده می‌کنند. تحقیقات تجربی و پیمایشی، از نمونه‌های بارز روش‌های تحقیق کمی می‌باشند. در مقابل، روش‌های کیفی شامل جمع‌آوری و تحلیل داده‌های غیر عددی مانند متن‌ها، مصاحبه‌ها و مشاهده‌ها هستند. تحقیقات زمینه‌یابی و تحلیل محتوا از نمونه‌های این روش‌ها می‌باشند (حافظ نیا، ۱۳۸۶).

در این مطالعه از روش تحقیق کیفی با استفاده از گروه کانونی برخط بهره گرفته شد. هدف از این جلسات بررسی نقش هوش مصنوعی در امنیت عمومی بود. گروه کانونی روشی است که به محققان اجازه می‌دهد تا از طریق بحث‌های گروهی به درک عمیق‌تری از دیدگاه‌ها، تجارب و نگرانی‌های شرکت‌کنندگان دست یابند. این روش امکان تبادل آزادانه نظرات را فراهم می‌کند و به دلیل تعامل مستقیم میان شرکت‌کنندگان، باعث پویایی و غنای بیشتر بحث‌ها می‌شود (پلامر-دآماتو، ۲۰۰۸). استفاده از گروه کانونی به عنوان روش تحقیق در این مطالعه، به دلیل فراهم آوردن محیطی تعاملی و پویا، منجر به استخراج داده‌های غنی و چندبعدی شد. این روش، برخلاف مصاحبه‌های فردی، امکان مشاهده و تحلیل تعاملات و پویایی‌های گروهی را فراهم می‌کند، که خود به درک عمیق‌تر و چندلایه‌ای از موضوع منجر می‌شود. علاوه بر این، تنوع دیدگاه‌ها در گروه،



فرصت بحث‌های جامع‌تر و متنوع‌تری را به وجود آورد که به شناسایی چارچوب‌های پیاده‌سازی هوش مصنوعی در امنیت عمومی کمک می‌کند.

گروه کانونی این تحقیق شامل شش نفر از متخصصین حوزه فناوری اطلاعات و سیستم‌های اطلاعاتی بود: چهار مدیر فناوری اطلاعات و دو تحلیلگر سیستم. انتخاب این افراد بر اساس تخصص و تجربه آن‌ها در زمینه هوش مصنوعی و آشنایی با مباحث حوزه امنیت عمومی صورت گرفت تا اطمینان حاصل شود که دیدگاه‌های مطرح‌شده دارای عمق علمی و عملی کافی هستند. خبرگان معمولاً توانایی شناسایی روندهای جدید و پیش‌بینی آینده را دارند. در حوزه امنیت عمومی و هوش مصنوعی، این اطلاعات می‌تواند بسیار ارزشمند باشد. به عنوان مثال، یک متخصص هوش مصنوعی می‌تواند پیش‌بینی کند که چگونه تکنولوژی‌های جدید می‌توانند بر امنیت عمومی تأثیر بگذارند و چه تهدیدات جدیدی ممکن است ظهور کنند. این اطلاعات می‌تواند به سیاست‌گذاران و مدیران امنیتی کمک کند تا استراتژی‌های مناسبی برای آینده تدوین کنند. اطلاعات دقیق‌تری در مورد سن و سابقه کاری این افراد در جدول ۱ ارائه شده است.

جلسه اول با ارائه خلاصه‌ای از ادبیات موضوع توسط اداره کننده جلسه، آغاز شد تا شرکت‌کنندگان با زمینه علمی بحث آشنا شوند. سپس پرسش کلیدی «مهمترین نقش هوش مصنوعی در امنیت عمومی چیست؟» مطرح شد و بحث آغاز گردید. این پرسش به عنوان محرکی برای شروع گفتگو عمل کرد و پس از آن، بحث به صورت آزاد پیش رفت تا شرکت‌کنندگان بتوانند نظرات خود را به شکل کاملاً باز و بدون محدودیت در قالب سه جلسه بر گزار شده، بیان کنند.

در طول جلسات، یادداشت‌برداری دقیقی از تمامی نظرات و دیدگاه‌ها انجام شد و جمع‌بندی اولیه در انتهای هر جلسه صورت پذیرفت. در نهایت، برای تحلیل داده‌ها، از روش کدگذاری استفاده گردید. کدگذاری به معنای برچسب‌گذاری و دسته‌بندی داده‌های کیفی است که به شناسایی الگوها و تم‌ها در بحث کمک می‌کند. این کدها سپس با ادبیات موضوعی تطبیق داده شدند تا همخوانی و تضادهای موجود بین دیدگاه‌های شرکت‌کنندگان و مفاهیم نظری شناسایی شوند.



جدول ۱- مشخصات متخصصان هوش مصنوعی فعال در حوزه امنیت

ردیف	سمت سازمانی	سابقه کاری (سال)	سن
۱	مدیر فناوری اطلاعات	۱۵-۱۰	۴۰-۵۰
۲	مدیر فناوری اطلاعات	۱۵-۱۰	۴۰-۵۰
۳	مدیر فناوری اطلاعات	۱۵-۱۰	۴۰-۳۰
۴	مدیر فناوری اطلاعات	۲۰-۱۵	۶۰-۵۰
۵	تحلیلگر سیستم‌های اطلاعاتی	۱۰-۵	۴۰-۳۰
۶	تحلیلگر سیستم‌های اطلاعاتی	۱۵-۱۰	۴۰-۵۰

تجزیه و تحلیل

بر اساس تحلیل مطالب ارائه شده در گروه کانونی نقش هوش مصنوعی به عنوان یک فناوری تحول آفرین از پنج طریق مشخص و قابل بحث است، که در ادامه به تشریح هر یک پرداخته شده است.

پشتیبانی از تصمیم‌گیری: هوش مصنوعی می‌تواند به کارکنان فعال در حوزه امنیت عمومی در اتخاذ تصمیمات آگاهانه کمک کند و با ارائه بینش‌های فوری، توصیه‌ها و تحلیل سناریوها بر اساس داده‌های موجود، به بهبود کارایی تصمیم‌گیری کمک کند. این سیستم‌ها معمولاً دارای داشبوردهایی هستند که اطلاعات و داده‌های مربوط به تهدیدات و وضعیت‌های اضطراری را به شکلی قابل فهم و آنی نمایش می‌دهند. این اطلاعات می‌تواند شامل نمودارها، نقشه‌ها و تحلیل‌های آماری باشد. همچنین سیستم‌های پشتیبانی از تصمیم‌گیری اغلب از شبیه‌سازی‌های سناریویی استفاده می‌کنند تا اثرات احتمالی انتخاب‌های مختلف را بررسی کنند. به عنوان مثال، در صورت وقوع یک حادثه طبیعی، سیستم می‌تواند شبیه‌سازی کند که انسداد برخی جاده‌ها چه اثری بر زمان پاسخگویی تیم‌های اورژانس خواهد داشت. هوش مصنوعی می‌تواند با تحلیل داده‌های تاریخی و یافته‌های گذشته، توصیه‌هایی برای مدیریت بحران ارائه دهد. به عنوان مثال، ارائه راهکارهایی برای بسیج نیروها در مناطق پرخطر یا بهره‌برداری از منابع بهینه.

ارتقاء توان پیش‌بینی و کنترل پیش‌نگر: تحلیل پیش‌بینی مبتنی بر هوش مصنوعی می‌تواند



به شناسایی الگوها، روندها و تهدیدات بالقوه کمک کند و به نیروهای امنیتی و سازمان‌های فعال در حوزه امنیت عمومی امکان می‌دهد به صورت پیشگیرانه با مسائل نوظهور برخورد کنند. با استفاده از تحلیل پیش‌بینی، سیستم‌های هوش مصنوعی می‌توانند مناطق با نرخ بالای وقوع جرم را شناسایی کرده و به نیروهای امنیتی اطلاعاتی در مورد زمان و مکان احتمالی وقوع جرایم بعدی بدهند. این امر به تخصیص بهتر منابع و اجرای پروتکل‌های پیشگیرانه منجر می‌شود. همچنین با تحلیل داده‌های رفتاری و تاریخچه جرایم، هوش مصنوعی می‌تواند الگوها و نشانه‌هایی از رفتار مجرمان را شناسایی کند. این امر می‌تواند به پیشگیری از جرایم برنامه‌ریزی شده و جلوگیری از تکرار جرم توسط مجرمان تحت نظر کمک کند. در نهایت، تحلیل پیش‌بینی می‌تواند به شناسایی تهدیدات امنیتی بزرگ‌تر، نظیر حملات تروریستی یا ناآرامی‌های مدنی کمک کند. با تحلیل داده‌های رسانه‌های اجتماعی، اطلاعات استخباراتی و سایر منابع داده، تکنیک‌های پیش‌بینی می‌توانند به شناسایی الگوها و نشانه‌های اولیه این تهدیدات پرداخته و اقدامات فوری را توصیه کنند.

نظارت و پایش خودکار: سیستم‌های مبتنی بر هوش مصنوعی می‌توانند حجم عظیمی از داده‌ها را از منابع مختلف مانند دوربین‌های نظارتی، شبکه‌های اجتماعی و شبکه‌های حسگر تحلیل کنند تا فعالیت‌های مشکوک را شناسایی و به طور مؤثرتری پاسخ دهند. یکی از کاربردهای مهم هوش مصنوعی در نظارت، استفاده از الگوریتم‌های تشخیص چهره است. این الگوریتم‌ها می‌توانند چهره افراد را در تصاویر و ویدئوها شناسایی کرده و با پایگاه داده‌های شناخته شده تطبیق دهند. این فناوری به شناسایی و دستگیری مجرمانی که در فهرست‌های تحت تعقیب هستند کمک می‌کند. سیستم‌های هوش مصنوعی همچنین می‌توانند رفتارهای غیرعادی را به لحظه از طریق دوربین‌های نظارتی تشخیص دهند. به عنوان مثال، رفتارهایی مانند ترک کردن کیفی در مکان عمومی یا تجمع خطرناک افراد می‌توانند به سرعت شناسایی و اخطار داده شوند. حسگرهای مختلفی مانند میکروفون‌ها، حسگرهای حرکتی و حتی حسگرهای شیمیایی به سیستم‌های نظارت کمک می‌کنند. هوش مصنوعی می‌تواند داده‌های این حسگرها را تحلیل کرده و رفتارهای مشکوک یا تهدیدات محیطی را متوجه شود.

بهینه‌سازی منابع: هوش مصنوعی می‌تواند به بهینه‌سازی تخصیص و استقرار منابع در برای ارتقای امنیت عمومی مانند پرسنل، تجهیزات و پاسخ‌های اضطراری کمک کند تا کارایی و اثربخشی کلی بهبود یابد. در طرح‌های عملیاتی با استفاده از تکنیک‌های یادگیری ماشین، می‌توان



پیش‌بینی کرد که چه تعداد نیرو و تجهیزات در یک منطقه خاص لازم است و آن‌ها را به طور بهینه تخصیص داد. این امر می‌تواند به کاهش هزینه‌ها و افزایش کارایی کمک کند. در مواقع اضطراری، هوش مصنوعی می‌تواند بر اساس داده‌های ترافیکی و تحلیل به لحظه، بهترین مسیرها برای خودروهای اورژانسی را پیشنهاد دهد و حتی سیستم‌های ترافیکی را بهینه‌سازی کند تا مسیرها برای عبور آزاد باشند. و با این موضوع که هوش مصنوعی می‌تواند در برنامه‌ریزی شیفت‌ها و توزیع نیروی انسانی بر اساس نیازهای زمانی و مکانی نقش داشته باشد. این امر به کارآمدی و بهره‌وری بیشتر کارکنان امنیتی کمک می‌کند.

افزایش تعامل با شهروندان: چت‌بات‌ها و دستیارهای مجازی مبتنی بر هوش مصنوعی می‌توانند تعامل با شهروندان را بهبود بخشند و اطلاعات به موقع، مکانیزم‌های گزارش‌دهی و کمک‌های شخصی‌سازی شده در طول رویدادهای اضطراری یا ایمنی عمومی ارائه دهند. این ابزارها می‌توانند در مواقع اضطراری بی‌وقفه به شهروندان کمک کنند تا منابع و اطلاعات مورد نیاز خود را بیابند. شهروندان می‌توانند از طریق سیستم‌های گزارش‌دهی خودکار، مشکلات و اضطراری‌هایی که با آن‌ها مواجه هستند را به سرعت گزارش دهند و نیازهای خود را منتقل کنند. این سیستم‌ها می‌توانند به سرعت اطلاعات را به مسئولان مربوطه منتقل کنند. هوش مصنوعی می‌تواند با تحلیل داده‌های شهروندان، خدمات شخصی‌سازی شده‌تری مانند توصیه‌های ایمنی در مواقع خاص یا اطلاعات مربوط به تهدیدات محلی را ارائه دهد. با ادغام فناوری‌های هوش مصنوعی در سیستم‌ها و عملیات امنیت عمومی، دولت‌ها و سازمان‌های مسئول در اجرای قانون می‌توانند قابلیت‌های خود را برای پیشگیری، شناسایی و پاسخ به تهدیدات مختلف بهبود بخشند و در نهایت ایمنی و امنیت عمومی را ارتقا دهند.

نتیجه‌گیری

هوش مصنوعی به عنوان یکی از پیشرفته‌ترین فناوری‌های عصر حاضر، می‌تواند نقش بسیار مهمی در بهبود امنیت عمومی ایفا کند. این فناوری با توانایی‌های منحصر به فرد خود در پردازش و تحلیل داده‌ها، شناسایی الگوها و پیش‌بینی وقایع آینده، می‌تواند به دستگاه‌های امنیتی کمک کند تا با دقت و سرعت بیشتری به تهدیدات پاسخ دهند. بر اساس مطالعات مرور شده و یافته‌های حاصل از جلسات آنلاین گروه کانونی، این فناوری، با استفاده از قابلیت‌های گسترده خود در تجزیه و تحلیل داده‌ها و پردازش سریع اطلاعات، به طور چشمگیری از شش طریق تصمیم‌گیری دقیق‌تر



و سریعتر، نظارت و پایش بهتر، مدیریت بحران فعال، هماهنگی ارتباطی مؤثرتر، تخصیص بهتر منابع و خودکارسازی فرآیندها به تحقق امنیت عمومی کمک می‌کند.

یافته‌های این تحقیق می‌تواند مبنای ایجاد نظریه‌های جدید و مدل‌های مفهومی در این حوزه باشد. مقاله ممکن است به طراحی چارچوب‌های نظری جدیدی برای تحلیل و ارزیابی کاربردهای هوش مصنوعی در امنیت عمومی کمک نماید. بر اساس یافته‌های پژوهش پیشنهاد می‌شود که دستگاه‌های امنیتی و نهادهای مربوطه از فناوری‌های هوش مصنوعی برای بهبود دقت و سرعت در شناسایی تهدیدات و پاسخ به آن‌ها بهره‌برداری کنند. این شامل استفاده از الگوریتم‌های پیشرفته برای تحلیل داده‌ها و پیش‌بینی وقایع است. به کارگیری سیستم‌های هوش مصنوعی برای نظارت و پایش مداوم محیط‌های حساس و کلیدی می‌تواند به بهبود قابلیت‌های پیشگیرانه و واکنش سریع به تهدیدات کمک کند. پیشنهاد می‌شود که از ابزارهای هوش مصنوعی برای بهبود مدیریت بحران و هماهنگی ارتباطات در زمان وقوع حوادث استفاده شود. این ابزارها می‌توانند به تسهیل ارتباطات و تخصیص منابع بهینه در شرایط اضطراری کمک کنند. تمرکز بر این موضوع که با استفاده از هوش مصنوعی برای تحلیل و پیش‌بینی نیازهای امنیتی، می‌تواند منابع را به‌طور مؤثرتری تخصیص داد و از هدررفت منابع جلوگیری کرد، می‌تواند نتایج مثبتی در افزایش کارایی داشته باشد. پیاده‌سازی سیستم‌های هوش مصنوعی برای خودکارسازی فرآیندهای امنیتی، نظیر تحلیل داده‌ها و گزارش‌دهی، می‌تواند به کاهش بار کاری و افزایش کارایی در عملیات امنیتی منجر شود. این پیشنهادها می‌تواند به بهبود عملکرد و کارایی سیستم‌های امنیتی کمک کرده و بهره‌برداری مؤثرتر از فناوری هوش مصنوعی در راستای ارتقاء امنیت عمومی را تسهیل کند. هوش مصنوعی به‌عنوان یک ابزار قدرتمند می‌تواند به بهبود امنیت عمومی و ملی کمک کند، اما استفاده مؤثر از آن نیازمند برنامه‌ریزی، مدیریت و نظارت دقیق است. با اتخاذ رویکردهای مناسب و ایجاد چارچوب‌های قانونی و راهبردی مناسب، می‌توان از ظرفیت‌های هوش مصنوعی به بهترین شکل ممکن بهره‌برداری کرد و امنیت عمومی را به‌طور قابل توجهی بهبود بخشید.

با توجه به اهمیت موضوع، بدیهی است که تحقیقات بیشتری برای تحلیل چگونگی تأثیر هوش مصنوعی بر مقابله با تهدیدهای مختلف امنیتی، از جمله تهدیدات سایبری، تروریسم و جرایم سازمان‌یافته، لازم است. بررسی جداگانه چهار روش استفاده از هوش مصنوعی (هوانگ و راست^۱،



۲۰۱۸)، یعنی هوش مکانیکی^۱ (توانایی انجام کارهای عادی و تکراری)، هوش تحلیلی^۲ (توانایی پردازش اطلاعات برای حل مسئله و یادگیری)، هوش شهودی^۳ (توانایی تفکر خلاقانه و سازگاری موثر با موقعیت‌های جدید)، و هوش همدلانه^۴ (توانایی تشخیص و درک احساسات، پاسخ مناسب عاطفی و تاثیرگذاری بر دیگران) در امنیت عمومی، می‌تواند نتایج مفیدی به دنبال داشته باشد. مطالعات آینده می‌توانند به بررسی و تحلیل چالش‌های اخلاقی و مسائل حریم خصوصی مرتبط با استفاده از هوش مصنوعی در امنیت عمومی پرداخته و راهکارهایی برای مدیریت این چالش‌ها ارائه دهند. به طور خاص برای ارتقاء امنیت عمومی کشور، پیشنهاد می‌شود در مطالعات بعدی به تحلیل تجربیات و پیاده‌سازی‌های بین‌المللی هوش مصنوعی در حوزه امنیت عمومی پرداخته شود، تا از این طریق بهترین شیوه‌های جهانی برای بهبود امنیت عمومی کشور مناسب‌سازی گردد. جلسات گروه کانونی ممکن است تحت تأثیر نظرات یا تعصبات خاص شرکت‌کنندگان قرار گیرند، که می‌تواند بر تنوع و دقت نتایج تأثیر بگذارد. همچنین این پژوهش در زمانی محدود انجام شده است که زمان محدود برای انجام تحقیق و تحلیل نتایج ممکن است باعث شده باشد که برخی جنبه‌ها و جزئیات مهم در بررسی کاربردهای هوش مصنوعی نادیده گرفته شوند. و در نهایت پیشرفت‌های سریع در فناوری هوش مصنوعی ممکن است نتایج تحقیق را به سرعت منسوخ کند و تحقیقات جدیدتری نیاز باشد تا تغییرات و پیشرفت‌های جدید را در نظر بگیرد. تمامی این محدودیت‌ها موضوعاتی است که باید در مطالعات بعدی مد نظر قرار گیرد.

-
- 1 Mechanical
 - 2 Analytical
 - 3 Intuition
 - 4 Empathetic

منابع

۱. احمدی، علی - زرگر، افشین و آدمی، علی (۱۴۰۲). فناوری هوش مصنوعی و تغییر در امنیت ملی دولت‌ها. سیاست دفاعی. ۳۲(۱۲۳)
۲. بابائیان، فاطمه - صفدری رنجبر، مصطفی و حکیم، امین (۱۴۰۲). واکاوی نقش هوش مصنوعی در چرخه سیاست گذاری عمومی؛ رویکرد فراترکیب، <https://civilica.com/doc/1756581/>
۳. حافظ نیا، محمدرضا (۱۳۸۶). مقدمه‌ای بر تحقیق در علوم انسانی، تهران انتشارات سمت.
۴. خاکی، غلامرضا (۱۳۹۱). روش تحقیق (بارویکرد پایان نامه نویسی) تهران انتشارات فوژان، چاپ سوم.
۵. دانایی فرد، حسن (۱۴۰۱). هوش مصنوعی و کشورداری: واکاوی دستاوردها، مطالعات مدیریت دولتی ایران دوره پنجم شماره ۴.
۶. نمکی، مهدی. فرشید بی باک، علی ابراهیمی (۱۴۰۲). آینده پژوهی اقدامات دشمنان با تاکید بر هوش مصنوعی علیه امنیت پایدار کشور، نشریه دانش انتظامی آذربایجان غربی، ۱۶(۵۹)، ۱۶-۲۱
44magiran.com/p2656961-21
7. Arruda, S. M. P., Brito, P. A., Akai, L. M. C., & Cavalcante, A. V. (2024). Mapping the future of public security, justice and the law enforcement: A bibliometric perspective on prospective analysis. *Brazilian Journal of Law, Technology and Innovation*, 2(1), 90-119.
8. Baldwin, D. A. (1997). "The Concept of Security." *Review of International Studies*, 23(1), 5-26
9. Gil de Zúñiga, H., Goyanes, M., & Durotoye, T. (2024). A scholarly definition of artificial intelligence (AI): advancing AI as a conceptual framework in communication research. *Political communication*, 41(2), 317-334.
10. Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, 61(4), 5-14.
11. Hejduk, M. (2020). Public Security and its Contexts. *Internal Security*, 12, 55-68.



12. Kelly, S., Kaye, S. A., & Oviedo-Trespalacios, O. (2023). What factors contribute to the acceptance of artificial intelligence? A systematic review. *Telematics and Informatics*, 77, 101925.
13. Lawelai, H., Iswanto, I., & Raharja, N. M. (2023). Use of Artificial Intelligence in Public Services: A Bibliometric Analysis and Visualization. *TEM Journal*, 12(2), 798.
14. Ning, W. (2023). A Legal and Ethical Review of Artificial Intelligence Technology in Public Safety Management. *Applied Mathematics and Nonlinear Sciences*, 9(1).
15. Poleto, T., Nepomuceno, T. C. C., De Carvalho, V. D. H., Friaes, L. C. B. D. O., De Oliveira, R. C. P., & Figueiredo, C. J. J. (2023). Information security applications in smart cities: A bibliometric analysis of emerging research. *Future Internet*, 15(12), 393.
16. Reese, S. (2012). "Homeland Security: A Framework for Addressing the Nation's Issues." *Congressional Research Service*
17. Slayer, K. M. (2020). Artificial intelligence and national security. *Congressional Research SVC Washington United States*.
18. Walt, S. M. (1991). The renaissance of security studies. *International studies quarterly*, 35(2), 211-239.
19. Wamba, S. F., Bawack, R. E., & Carillo, K. D. A. (2019). The state of artificial intelligence research in the context of national security: bibliometric analysis and research agenda. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18* (pp. 255-266). Springer International Publishing.
20. Mahor, V., Rawat, R., Kumar, A., Garg, B., & Pachlasiya, K. (2023). IoT and artificial intelligence techniques for public safety and security. In *Smart urban computing applications* (pp. 111-126). River Publishers.
21. Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A. X.





- (2015). From physical security to cybersecurity. *Journal of Cybersecurity*, 1(1), 19-35.
22. Aldis, W. (2008). Health security as a public health concept: a critical analysis. *Health Policy and Planning*, 23(6), 369-375.
23. Gonzalez-Eiras, M., & Niepelt, D. (2008). The future of social security. *Journal of monetary Economics*, 55(2), 197-218.
24. Plummer-D'Amato, P. (2008). Focus group methodology Part 1: Considerations for design. *International Journal of Therapy and Rehabilitation*, 15(2), 69-73.
25. Huang, Ming-Hui, and Roland T. Rust. "Artificial intelligence in service." *Journal of service research* 21, no. 2 (2018): 155-172.
26. Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & management*, 58(3), 103434.