Quarterly Journal of Defense Technology Engineering Imam Ali University
Summer 2025, Vol. 42

Original Research

Artificial intelligence in emerging technologies and its security

Seyed Roohollah Mirakbari [1], Alireza Rezaei[2], Mojtaba lak[3], Mehrdad Kamarabi[4]

[1,2,3] Flight and Engineering Department, Imam Ali University

ARTICLE INFO

Received: 2025.06.26
Accepted: 2025.08.01
Published: 2025.09.06

Keyword:
Artificial intelligence, emerging technology, security

***Corresponding Author:**
Seyed Roohollah Mirakbari
Email:
rooh_mir2003@yahoo.com

ABSTRACT

Due to the enormous potential of artificial intelligence in modern warfare, many of the most powerful countries in the world have increased their investments in their military and security. Considering that artificial intelligence will soon play an ever-increasing role in military affairs, practically like all other aspects of our lives, Probably, as time passes, the role of humans will decrease even more in atomic decision-making. In fact, in the future where artificial intelligence covers the whole world, the human role may disappear completely and machines will be left alone to decide the fate of humans.

The future war is associated with artificial intelligence technology and we should not neglect this area. The design and application of information principles, methods, measures and arrangements are considered in combat and information operations, which, although their observance and application may not guarantee a definite victory, but not paying attention and not observing them will definitely lead to failure and failure. will have. Therefore, it is necessary that all stages of military and intelligence activities, in different fields of the future war environment, in land, air, space, sea and cyberspace, should be carried out in the context of information attitude and belief in the necessity of observing security principles and measures in order to achieve the goals. A strategy and victory can be achieved with a higher certainty factor**.** This includes the use of security measures, encryption and monitoring of artificial intelligence information, which we discuss in this research.

فصل نامه مهندسی فناوری‌های دفاعی دانشگاه افسری امام علی (ع)

تابستان 1404 ، دوره 42

مقاله پژوهشی

هوش مصنوعی در فناوری‌های نوظهور و امنیت آن

سید روح اله میراکبری[1] *، علیرضا رضایی [2]، مجتبی لک [3]، مهرداد کمرآبی [4]

1و2و3 و 4 - مدرس، دانشکده مهندسی و پرواز، دانشگاه امام علی (ع)

اطلاعات مقاله

دریافت مقاله: 1404/04/05

پذیرش مقاله: 1404/05/10

انتشار مقاله: 1404/06/15

کلید واژگان:

هوش مصنوعی،

فناوری نوظهور، امنیت

*نویسنده مسئول

سید روح اله میراکبری

پست الکترونیکی:

rooh_mir2003@yahoo.com

چکیده

با توجه به توانایی عظیم هوش مصنوعی در جنگ مدرن، بسیاری از قدرتمندترین کشورها در جهان سرمایه گذاری های خود را برای ارتش و امنیت خود افزایش داده اند. با توجه به اینکه به زودی هوش مصنوعی عملا همچون تمام دیگر شئون زندگی ما، نقشی همواره فزاینده در امور نظامی ایفا خواهد کرد، احتمالا هر چه می گذرد نقش انسان ها حتی در تصمیم گیری های اتمی بیشتر تقلیل خواهد یافت. در واقع در آینده ای که هوش مصنوعی سراسر جهان را فرا گرفته، ممکن است نقش انسانی به کلی ناپدید شود و ماشین ها به حال خود گذاشته شوند تا برای سرنوشت انسان تصمیم بگیرند. جنگ آینده همراه با فناوری هوش مصنوعی همراه بوده و و از این حوزه نباید غافل شویم. طراحی و به‌کارگیری اصول، شیوه‌ها، تدابیر و تمهیدات اطلاعاتی در عملیاتهای رزمی و اطلاعاتی به شمار رفته که رعایت و به کارگیری آن هر چند ممکن است پیروزی قطعی را تضمین ننماید اما به طور قطع عدم توجه و رعایت نکردن آن ناکامی و شکست حتمی را درپی خواهد داشت. بنابراین ضروری می نمایدکه تمام مراحل فعالیتهای نظامی و اطلاعاتی، در عرصه های مختلف محیط جنگ آینده، در زمین، هوا، فضا، دریا و فضای سایبری، در بستر نگرش اطلاعاتی و باور به ضرورت رعایت اصول و تمهیدات امنیتی انجام پذیرد تا دستیابی به اهداف راهبردی وکسب پیروزی با ضریب قطعیت بیشتری میسور گردد. این شامل استفاده از اقدامات امنیتی، رمزگذاری و نظارت بر اطلاعات هوش مصنوعی است که در این تحقیق به ان می‌پردازیم.

1- مقدمه

هوش مصنوعی (AI[1]) یک شاخه از علوم کامپیوتر است که به ایجاد هوش در ماشین‌ها می‌پردازد. هوش مصنوعی شامل مجموعه‌ای از تکنیک‌ها و الگوریتم‌هایی است که به ماشین‌ها امکان می‌دهد تا یاد بگیرند، فکر کنند و عمل کنند. منظور از این مفهوم، ماشینی است که همانند انسان فکر کند و توانایی تقلید رفتار انسان را داشته باشد. چنین ماشینی می‌تواند وظایفی را انجام دهند که به هوش انسانی نیاز دارد. با پیشرفت علم و تکنولوژی روزبه‌روز هوش مصنوعی توسعه می‌یابد و دستگاه‌ها و ماشین‌ها و نرم‌افزارها در حوزه‌های مختلفی چون پزشکی، نظامی، امنیتی، اینترنت، خودروسازی و بسیاری دیگر وارد شده و این حوزه‌ها را دستخوش تغییر و تحولات مثبتی کرده است. استفاده از هوش مصنوعی در حوزه نظامی از اوایل این دهه میلادی در بین ملت‌ها به‌صورت رقابت درآمده و باعث پیشرفت و توسعه نسل جدید تسلیحات و تجهیزات نظامی، از جمله بمب‌های هوشمند با هدایت لیزر و یا پهپادها و هواپیماهای رادار گریز شده است و هر کشوری سعی دارد با به‌کارگیری آن در تجهیزات دفاعی و ادوات نظامی خود، در این زمینه پیشرو شده و در صورت هرگونه تهدید، به مقابله با آن بپردازد. مخاطراتی که از ناحیه تهدیدات و آسیب‌پذیریهای اطلاعاتی در جنگ‌های احتمالی آینده نیروهای مسلح را مورد تهدید قرار می‌دهد، تدوین راهبردها و طراحی شیوه‌های تاکتیکی و اصول و قواعد نوین اطلاعاتی را دوچندان می‌نماید (Singer, 2014)

رای مقابله با تلاش‌های مضاعف اطلاعاتی دشمن، دستگاه‌های امنیتی رسالت و وظیفه دارند تا با کسب آگاهی و شناخت کافی از اهداف و شیوه‌های نفوذ و جمع‌آوری دشمن و با به کارگیری تجهیزات و بهره‌گیری از فناوری‌های پیشرفته روز به مقابله با اقدامات جمع‌آوری، نفوذ و جاسوسی دشمن پرداخته، او را در دست یابی به اهدافش ناکام گذارد یا در رسیدن دشمن به مقاصد موردنظر مانع جدی ایجاد و امکان هرگونه توفیق برای دشمن در راستای جمع‌آوری اخبار و اطلاعات را بسیار سخت، پرهزینه و پر دردسر نماید، تا بدین طریق بستر لازم برای امکان برقراری امنیت مؤثر از اطلاعات و به‌کارگیری مناسب، به موقع و مؤثر توان رزم نیروهای خودی علیه دشمن و همچنین کاهش قابلیت‌های نیـروهای دشمن در به‌کارگیری مؤثر توان رزمـی علیه نیروهای خودی فراهم گردد. نقش فناوری های نوین اطلاعاتی در جنگ های آینده جهت صیانت و حفاظت از یگان‌ها، طرح‌های عملیاتی و مأموریت‌های فرماندهی در عرصه جنگ احتمالی آینده با دشمنی که به لحاظ اطلاعات، فناوری و ابزار و تجهیزات در حوزه‌های مختلف «هوا، فضا، زمین و دریا» در سطح جهانی از برتری نسبی برخوردار می‌باشد ضرورتی انکار ناپذیر به شمار می رود.

هوش مصنوعی به عنوان یکی از برترین فناوری های نوظهور، زمانی اتفاق می‌افتد که یک دستگاه کاملا از اعمال خود آگاه شود، توانایی خردمندی را داشته باشد، بتواند اطلاعات را ذخیره کند، یاد بگیرد، تصمیم بگیرد و ابتکار عمل خود را داشته باشد.

در مقایسه با سیستم های مرسوم ، مؤسسات نظامی که حجم عظیمی از داده ها را به خود می گیرند ، قادر به ادغام هوش مصنوعی در یک فرایند یکپارچه تر هستند. تضمین بهره وری عملیاتی ، هوش مصنوعی بهبود خود تنظیم ، خودکنترلی و عملکرد خود سیستم های جنگی ، اعتبار به محاسبات ذاتی خود همراه با قابلیت

[1] Artificial intelligence

تصمیم گیری دقیق است. برای بهکارگیری این مفاهیم اساسی در جنگهای اینده، باید تأثیر محصولات جانبی پیچیده تکنولوژی را نیز در نظر گرفت. از ساخته شدن نفربرهای هوایی و زیردریاییهای هسته‌ای گرفته تا پیشرفتهای رخداده در صعنت هوانوردی و طراحی هواپیماهای بدون سرنشین و خودروهای تاکتیکی فوق سبک تا رشد فعالیتهای فضایی و فضای سایبری همگی تأثیر زیادی بر استراتژی و ویژگیهای جنگ داشته‌اند، اما ماهیت اساسی جنگ را تغییر ندادهاند. پیشرفت تکنولوژی در سیستم‌های اطلاعاتی نیز باعث کاهش ابهامات موجود در جنگ شده، اما ساختار این دستگاهها باعث شکل‌گیری آسیب‌های جدیدی در سیستم عملکردی نیروهای نظامی شده‌است که به‌عنوان نمونه میتوان به گسترش حملات سایبری اشاره کرد (سید حسینی و همکاران ،1397).

2- سوال و اهداف پژوهش

1- رویکردها و مدل‌های هوش مصنوعی در علوم نوظهور به چه صورت می باشد؟

2-شاخه‌ها و سطوح هوش مصنوعی در علوم نوظهور به چه صورت می باشد؟

3- کاربردها و مزایای هوش مصنوعی چه اهدافی را دنبال می کند؟

4- یرای امنیت اطلاعات هوش مصنوعی در علوم نوظهور در برابر حملات روش مطمئن چیست؟

سرعت مدرن‌سازی نظامی و ظهور قابلیت‌های جدید ناشی از نوآوری‌های فناورانه، تأثیر قابل‌توجهی بر ماهیت جنگ و نحوه اجرای عملیات‌های نظامی، از جمله نقش اساسی فناوری ها، خواهد داشت. تحقیقات در خصوص فناوری های نوظهور در عرصه نظامی تقریباً به طور کامل بر روی نتایج جنگ‌های جنگی متمرکز بوده است. بطوریکه که تعداد فزاینده‌ای از فعالیت‌های تحقیقاتی علمی و عملی به سبک آزمایشگاهی نظامی و جنگی با هدف بررسی استفاده از رباتیک، فناوری اطلاعات و هوش مصنوعی صورت پذیرفته است. بدیهی است که جامعه پژوهشی می تواند از آینده نگری و فعال بودن در طول اولویت بندی فناوری های نوظهور و چالش های ناشی از آنها بر ضریب امینت دفاعی خود بهره مند شود. این کار باعث بروز اطمینان از اثر بخشی نقشه های جنگی آنها با در نظر گرفتن فناوری نوظهور و تکثیر آن در میدان نبرد می شود، بطوریکه باعث تغییرات در ماهیت و چگونگی بکار گیری فناوری های نوظهور در طرح ریزی عملیات های جنگی می شود (Billing, 2021)

3- بیان مسئله و ضرورت تحقیق

فناوری های نوظهور عرصه ای بسیار ناشناخته برای نحوه فرماندهان عملیاتی جنگ ها در میدان های نبرد می باشد. تاریخ نبردهای مهم در تاریخ نشان دهنده اثرگذاری قطعی در پیروزی نبردهای جنگی از سوی بکارگیری فناوری های نوظهور در عرصه نظامی می باشد. تحقیقات بخش های نظامی و غیر نظامی در حدوث و ظهور فناوری های نوین همیشه در محرمانگی خود صورت پذیرفته و برای مخاطبان عرصه های تجاری غیر نظامی و نظامی همیشه امری چالش برانگیز و تقریبا غیر ممکن بوده است. کسب اطلاعات همواره و در همه

دوران‌ها بویژه در عصر کنونی که با رشد روز افزون امنیت فناوری اطلاعات و ارتباطات مواجهیم از اهمیت زیادی برخوردار بوده و باعث برتری در بسیاری از زمینه‌ها می‌شود. تمام کشورها برای ادامه حیات خود نیازمند دسترسی به امنیت هوش مصنوعی هستند و برای این دسترسی از هیچ تلاشی فروگزار نیستند.

امنیت دفاعی پشتوانه محکمی برای سیاست‌های اقتصادی، فرهنگی و سیاسی کشور است. موقعیت، حساسیت کشور ایران و پیچیدگی‌های سیاست‌های جهان و تحولات جهانی و منطقه‌ای ایجاب می‌کند با درنظرگرفتن تهدیدات به سیستم‌های روز مجهز نموده و از فناوری‌های نوین هوش مصنوعی استفاده نماید.

4- تعیین و تعریف متغیرهای اصلی

4-1- هوش مصنوعی

هوش مصنوعی روشی نوین برای ساخت ابزارهایی هوشمند با الگوبرداری از هوش انسان می‌باشد. ابزاری که شبیه انسان فکر کند و به جای او تصمیم بگیرد. در حقیقت این فناوری همان ماشین برنامه‌نویسی شده به دست انسان است که با هدف سهولت در انجام امور روزمره طراحی شده است. بسیاری از افراد، هوش مصنوعی را همچون رباتی در نظر می‌گیرند که به صورت فیزیکی قابل مشاهده می‌باشد.

4-2- فناوری‌های نوظهور

فن آوری ها را می توان به عنوان "مجموعه ای از دانش نظری و عملی، دانش فنی، مهارت ها و مصنوعاتی که برای توسعه، تولید و ارائه ... محصولات و خدمات استفاده می شود" تعریف کرد. در صورتیکه واژه نوظهور در کنار فناوری با برداشت های متفاوتی استفاده می‌شود در حالیکه گاهی اوقات واژه "نوظهور" برای بررسی فناوری‌هایی که تحلیلگران بعنوان در حال ظهور بالقوه در آینده قلمداد می شود؛ گاهی اوقات دیگر "نو ظهوری" برای توصیف فناوری هایی استفاده می شود که به مرحله ای رسیده اند که می دانیم در آینده نزدیک در یک سیستم تسلیحاتی کاربرد پیدا خواهند کرد(James, 2018).

4-3- جنگ آینده

مهمترین ویژگیهای جنگ های آینده که بیشترین اثر را بر روی نوع دفاع دانش‌بنیان خواهند داشت به ترتیب عبارت‌اند از: تحول در جمع‌آوری، تبادل و پردازش اطلاعات؛ دانش و فناوری محور بودن؛ دقت و هوشمندی؛ اهمیت روزافزون فرماندهی و کنترل در جنگ آینده؛ و از طرف دیگر مهمترین ویژگی‌های دفاع دانش‌بنیان که بیشترین تأثیر را بر روی نوع تهدیدات آینده خواهند گذاشت به ترتیب عبارتند از: همه‌جانبه بودن دفاع، تکیه بر سامانه فرماندهی و کنترل هوشمند و یکپارچه با بهره‌گیری از سامانه‌های پشتیبانی از تصمیم و تأثیرمحور بودن.

4-4- رمزنگاری

رمزنگاری اطلاعات، روشی مناسب به منظور حفاظت از اطلاعات حساس است . بدین ترتیب، صرفا افراد مجاز قادر به دستیابی و استفاده از اطلاعات خواهند بود. دانش تغییر دادن متن پیام به کمک یک کلید رمزنگاری و یک الگوریتم رمزنگاری است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج متن اصلی از متن رمزشده باشد و شخصی که از یکی یا هردوی آن‌ها اطلاعی ندارد، نتواند به محتوای پیام دسترسی پیدا کند.

4-5- امنیت اطلاعات

اطلاعات هوش مصنوعی که کاربرد نظامی دارند باید بیشترین سطح امنیت را داشته باشد. در محیط‌های نظامی، حمله به اطلاعات هوش مصنوعی به دو گونه تقسیم می‌شوند: حملات استراتژیک و حملات تاکتیکی. در حملات استراتژیک می‌توان به اطلاعاتی نظیر موقعیت فرستنده و گیرنده و نقش هر کدام در شبکه دست یافت و در حملات تاکتیکی می‌توان به توپولوژی شبکه و ارتباط بین فرستنده و گیرنده دست یافت (Youssef,2023).

امنیت اطلاعات[1] مبتنی است بر تحقق سه ویژگی زیر است:

1- صحت: عدم دسترسی افراد غیرمجاز به اطلاعات

2- محرمانگی: عدم دستکاری اطلاعات توسط افراد یا نرم‌افزارهای غیرمجاز.

3-دسترس پذیری: دسترسی به اطلاعات توسط افراد مجاز در هر مکان و در هرزمان.

5- پویایی و تغییر پذیری در جنگ های آینده با رویکردهای هوش مصنوعی

در عصر فرا صنعتی شاهد وقوع جنگ هایی هستیم که به مراتب از جنگ های گذشته، خطرناکتر و مهلکتر است. علت آن به دو ویژگی خاصی برمی گردد که با امتزاج خود، صحنه جدیدی را در عصر کنونی رقم زده است. اولی پیشرفت شگفت آور فناوری و دیگری انفجار اطلاعات است که به شدت، دقت، وسعت، زمان، میزان تخریب، محیط درگیری و ... در جنگها تأثیر گذار بوده است. جنگ با بنه و مایه اطلاعات و با استفاده از فن آوری جدید جایگاه ویژه ای در جنگهای آینده به خود اختصاص داده است. جنگ اطلاعاتی با سطوح مختلف (جنگ فرماندهی و کنترل، جنگ برپایه اطلاعات، جنگ الکترونیک، جنگ روانی، جنگ هکرها، جنگ اطلاعاتی اقتصادی، جنگ سایبرنتیک و جنگ ادراکی) جامعه جهانی را تحت تأثیر خود قرار داده است. جنگ آینده جنگ بایت ها و بیت ها خواهد بود. جنگ های آینده بر آفندها و پدافندهای دیجیتال استوار بوده و محدود به مرزهای جغرافیایی نبوده و لزوماً به برتری منابع ملی و قومی وابسته نخواهد بود. این تغییر ممکن است تحولاتی پدید آورد که موجب شود گروه ها و ملت هایی که پیش از این, تهدیدی برای قدرت های جهانی به حساب نمی آمدند تبدیل به تهدیداتی بزرگتر از تسلیحات سنتی از جمله تسلیحات کشتار جمعی شوند. جنگ اطلاعاتی به

[1] Information Security

بازیگران این امکان را می دهد که بدون توسل به جنگ مسلحانه، به اهداف سیاسی و راهبردی خود دست یابند. در فضای مجازی، مرز بین نظامی و غیرنظامی و نیز فیزیکی و مجازی چندان روشن و شفاف نیست، از این رو قدرت یا از طریق دولت ها و یا بازیگران غیردولتی اعمال می شود. در کنار سایر میدان های سنتی نبرد مثل زمین، هوا، دریا و فضا باید فضای مجازی را (پنجمین میدان نبرد) دانست؛ جنگ اطلاعاتی از اجزای جدید این محیط چند بعدی استاما، کاملاً جدا از آن در نظر گرفته نمی شود. و این تنها گوشه ای از تهدیدات و پیامدهای جنگ اطلاعاتی است که در حال وقوع و گسترش است.

استوارت راسل و پیتر نورویگ، دانشمندان علوم کامپیوتر، چهار رویکرد مختلف را بررسی کردند که بـه‌طور تاریخی زمینه هوش مصنوعی را تعریف کرده‌اند. این رویکردها عبارتند از:

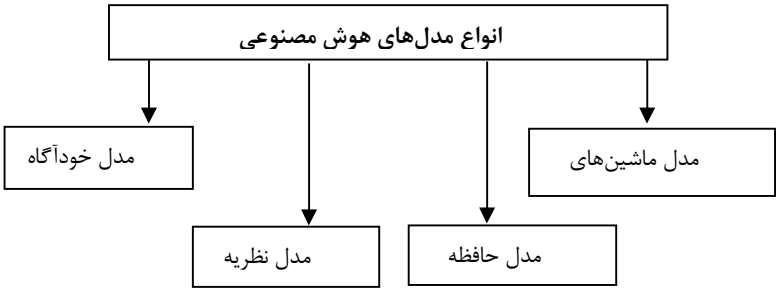
- انسانی فکر کردن
- منطقی فکر کردن
- انسانی عمل کردن
- منطقی عمل کردن

دو ایده اول، یعنی انسانی فکر کردن و منطقی فکر کردن، مربوط به فرایندهای تفکر و استدلال هستند؛ در حالی که دو مورد بعدی (انسانی عمل کردن و منطقی عمل کردن)، با رفتار سر و کار دارند. در این رویکردها، نورویگ و راسل، بر عوامل منطقی رسیدن به بهترین نتیجه تمرکز در جنگ‌های آینده دارند.

کشوری که فکر میکند دشمنانش سلاحهای مبتنی بر هوش مصنوعی دارند یا خواهند داشت، میخواهد با آنها مقابله کند. با این حال انتظار میرود استفاده گسترده از حملات سایبری مبتنی بر سیستمهای هوش مصنوعی همچنان چندان نزدیک نباشد. کشورها ممکن است با طرح محدود کردن مبارزات هوش مصنوعی مطرح شده در کنوانسیون دیجیتال ژنو موافقت کنند، با این حال اما این اقدام هم نمیتواند جلوی حملات سایبری مبتنی بر هوش مصنوعی را که از سوی گروههای مستقل، نظامیان و سازمانهای تروریستی و افراطیون انجام می‌شود، بگیرد. تقریبا واضح است که هوش مصنوعی در آیندهای نه چندان دور به عنوان سلاحی قدرتمند مورد استفاده قرار خواهد گرفت.

پیشرفتهای ایجاد شده در حوزه هوش مصنوعی می‌تواند علاوه بر کاربردهای نظامی، مزایای اقتصادی و تجاری زیادی برای کشورها داشته باشد، بنابراین در اختیار نداشتن سیستمهای هوش مصنوعی ممکن است ضررهای قابل توجهی به کشورها بزند. در اختیار داشتن این سیستمها همچنین میتواند توان دفاعی و بازدارندگی خوبی در مقابل حملات سایبری آینده به کشورها بدهد؛ درست مانند سلاحهای هستهای در زمان جنگ سرد.

6- انواع مدل‌های هوش مصنوعی



شکل 1: انواع مدل‌های هوش مصنوعی

هوش مصنوعی به چهار مدل کلی ماشین‌های واکنشی، حافظه محدود، نظریه ذهن و خود آگاهی تقسیم می‌گردد. هر یک از این مدل‌ها با توجه به هدف و قابلیت‌هایشان در حوزه‌های متعددی کاربرد دارند.

- مدل ماشین‌های واکنشی[1]

یکی از قدیمی‌ترین مدل‌های هوش مصنوعی، ماشین‌های واکنشی می‌باشد که تنها برای انجام وظایف تخصصی طراحی شده‌اند. این ماشین‌ها قادر به ذخیره اطلاعات نیستند. در نتیجه امکان تصمیم‌گیری بر اساس تجربیات گذشته را نداشته و تنها برای پاسخگویی به نیاز افراد ساخته شده‌اند. موتور جستجوی گوگل مثال خوبی برای این ویژگی می‌باشد.

- مدل حافظه محدود[2]

در این مدل، با کمک هوش مصنوعی امکان ذخیره اطلاعات و تصمیم‌گیری بر اساس داده‌های قبلی وجود دارد. در واقع اساس رفتار یک ماشین، سرنخ‌هایی است که در گذشته ارائه شده است. احراز هویت و شناسایی افراد در سامانه‌های مختلف از این نوع می‌باشند.

- مدل نظریه ذهن[3]

نظریه ذهن بدان معناست که هوش مصنوعی می‌تواند به شکل بهتری احساسات، عواطف و اعتقادات انسان‌ها را درک کند و سپس از این اطلاعات برای تصمیم‌گیری خود استفاده نماید. این شاخه از علم همچنان در حال توسعه می‌باشد و در صورت موفقیت آن تحول عظیمی در زندگی انسان‌ها رخ خواهد داد.

[1] Reactive Machines Model
[2] Limited Memory Model
[3] Theory of Mind Model

- مدل خود آگاه[1]

هدف از طراحی مدل خود آگاه، شبیه‌سازی مغز انسان می‌باشد. به شکلی که میزان درک یک ماشین به اندازه آگاهی و درک یک انسان باشد. در این فرضیه یک ربات، قدرت درک احساسات و نیاز دیگران را داشته و همانند یک انسان با آنان ارتباط برقرار خواهد کرد.

7- شاخه‌های هوش مصنوعی

در ایران هوش مصنوعی در حال توسعه است و در برخی از حوزه‌ها هم مورد استفاده قرار می‌گیرد؛ به‌عنوان‌مثال شرکت‌های ایرانی در حوزه تشخیص چهره توانستند سیستم‌های تشخیص چهره پیشرفته‌ای را تولید کنند که در سیستم‌های حضور و غیاب و امنیت استفاده می‌شود یا در حوزه تشخیص اجسام نیز پروژه‌هایی در دانشگاه‌ها و شرکت‌های فناوری ایران در حال انجام است.

علاوه بر این در حوزه رباتیک هم تحقیقات و پروژه‌هایی در دانشگاه‌ها و صنعت صورت می‌گیرد. برخی از شرکت هوش مصنوعی نیز ربات‌های هوشمندی را تولید کردند که قادر به تشخیص و پاسخ به محیط و وظایف مختلف هستند. در حوزه اقتصاد، هوش مصنوعی به تحلیل داده‌ها و پیش‌بینی رویدادها کمک می‌کند. برخی شرکت‌ها و مؤسسات تحقیقاتی در ایران توانستند الگوریتم‌های یادگیری ماشین را برای تحلیل داده‌های اقتصادی و مالی استفاده کنند. به‌طورکلی هوش مصنوعی در ایران هنوز در مراحل اولیه توسعه است و به سرمایه‌گذاری و تحقیقات بیشتری نیاز دارد (عظیم‌زاده، ح و همکاران ،1401).

7-1- رباتیک

ربات‌ها ماشین‌های برنامه ریزی شده‌ای هستند که به‌طور خودکار مجموعه‌ای از اقدامات پیچیده را انجام می‌دهند. افراد، ربات‌ها را با دستگاه‌های خارجی یا سیستم‌های کنترلی که درونشان تعبیه شده کنترل می‌کنند. ربات‌ها در انجام کارهای خسته کننده و تکراری کمک کننده هستند به ویژه ربات‌های مجهز به هوش مصنوعی که به شرکت‌هایی مانند ناسا در اکتشاف فضا کمک می‌کنند. ربات‌های انسان نما جدیدترین پیشرفت‌ها و نمونه‌های شناخته شده هستند؛ به‌عنوان‌مثال سوفیا رباتی است که توسط "Hanson Robotics" ساخته شده و با ترکیب هوش مصنوعی و شبکه‌های عصبی کار می‌کند. او چهره انسان‌ها را می‌شناسد و احساسات و ژست‌ها را درک می‌کند حتی می‌تواند با مردم تعامل داشته باشد.

7-2- تشخیص الگو

در این شاخه از هوش مصنوعی، الگوریتم‌ها و مدل‌هایی طراحی می‌شوند که قادر به تشخیص الگوهای خاص در داده‌ها هستند. این الگوریتم‌ها برای تشخیص الگوهای صوتی، تصویری، متنی و ... استفاده می‌شوند؛

[1] Self-aware Model

به‌عنوان‌مثال الگوریتم‌های تشخیص الگو در شناسایی چهره ویژگی‌های خاصی از صورت را شناسایی می‌کنند و افراد مختلف را تشخیص می‌دهند.

7-3- شبکه‌های عصبی مصنوعی

شبکه‌های عصبی به‌عنوان شبکه‌های عصبی مصنوعی (ANN[1]) یا شبکه‌های عصبی شبیه سازی شده (SNN[2]) هم شناخته می‌شوند. شبکه‌های عصبی از مغز انسان الهام می‌گیرند و نحوه ارسال سیگنال‌های نورون‌های بیولوژیکی به یکدیگر را کپی می‌کنند .شبکه‌های عصبی مصنوعی دارای لایه‌های گره‌ای هستند که از یک لایه ورودی، یک یا چند لایه پنهان و یک لایه خروجی تشکیل شدند. هر گره یک نورون مصنوعی نامیده می‌شود و به نورون‌های دیگر متصل می‌شود. هنگامی که خروجی یک گره فردی بیش از یک مقدار آستانه مشخص است، گره برای ارسال داده به لایه شبکه بعدی فعال می‌شود. شبکه‌های عصبی برای یادگیری و بهبود دقت به داده‌های آموزشی نیاز دارند.

7-4- یادگیری عمیق

یادگیری عمیق زیرمجموعه‌ای یادگیری ماشین است که شبکه‌های عصبی مصنوعی مغز انسان را با مهارت کامل تقلید می‌کند. در این صورت هوش مصنوعی وظایف استدلالی پیچیده را بدون دخالت انسان انجام می‌دهد.

7-5- تشخیص گفتار

در این شاخه سعی می‌شود تا برای تشخیص و تفسیر گفتار انسان الگوریتم‌ها و مدل‌هایی طراحی شوند. این الگوریتم‌ها به شناسایی کلمات و جملات مورد استفاده در یک گفتار کمک می‌کنند و در برخی موارد به ترجمه گفتار از یک زبان به زبان دیگر می‌پردازند.

7-6- پردازش زبان طبیعی

پردازش زبان طبیعی به رایانه‌ها اجازه می‌دهد تا هم متن و هم کلمات گفتاری را مانند انسان درک کنند. زبان‌شناسی و مدل‌های یادگیری عمیق، با ترکیب یادگیری ماشینی، زبان انسان را در داده‌های صوتی یا متنی پردازش می‌کنند تا معنی، هدف و احساسات رو کاملاً درک کنند؛ به‌عنوان‌مثال در تشخیص گفتار به متن، داده‌های صوتی به‌طور قابل اعتمادی به داده‌های متنی تبدیل می‌شوند. این کار خیلی چالش برانگیز است زیرا مردم با لحن، تأکید و لهجه‌های مختلف صحبت می‌کنند. برنامه نویسان باید برنامه‌های کاربردی مبتنی بر زبان طبیعی را به رایانه‌ها آموزش دهند تا بتوانند داده‌ها را از ابتدا درک کرده و تشخیص دهند. برخی از کاربردهای پردازش زبان طبیعی عبارت‌اند از:

---

[1] Artificial neural networks
[2] Simulated neural networks

- چت‌بات‌های مجازی که قادرند اطلاعات متنی را تشخیص دهند تا در طول زمان به مشتریان پاسخ‌های بهتری ارائه دهند.
- تشخیص هرزنامه‌ها که با پردازش زبان ایمیل‌ها آن‌ها را به بخش هرزنامه می‌فرستد.
- تحلیل احساسات و تجزیه و تحلیل زبان مورد استفاده در سیستم عامل‌های رسانه‌های اجتماعی که به استخراج احساسات و نگرش‌ها در مورد محصولات مختلف کمک می‌کند.

7-7- بینایی ماشین

یکی از محبوب‌ترین شاخه‌های هوش مصنوعی در حال حاضر «بینایی کامپیوتر» است. بینایی کامپیوتری به دنبال توسعه تکنیک‌هایی است که به رایانه‌ها در دیدن و درک تصاویر و فیلم‌های دیجیتال کمک می‌کند. استفاده از مدل‌های یادگیری ماشینی روی تصاویر به رایانه‌ها امکان می‌دهد اشیا، چهره‌ها، افراد، حیوانات و ... را شناسایی کنند.

مدل‌های الگوریتمی به رایانه‌ها کمک می‌کنند تا در مورد زمینه‌های داده‌های بصری آموزش ببینند و با داده‌های کافی که از طریق یک مدل تغذیه می‌شوند یک تصویر را از تصویر دیگر تشخیص دهند. یک شبکه عصبی کانولوشنال در کنار یک مدل کار می‌کند تا تصاویر را به پیکسل‌ها تجزیه کند و به آن‌ها برچسب بدهد؛ سپس شبکه عصبی از برچسب‌ها برای انجام کانولوشن که یک عملیات ریاضی روی دو تابع برای تولید تابع سوم است استفاده می‌کنند و پیش‌بینی‌هایی درباره آنچه می‌بیند انجام می‌دهند. بینایی کامپیوتر در صنایع مختلف کاربرد دارد.

8-7- شبکه عصبی

- شبکه عصبی پیچشی

این شاخه از هوش مصنوعی برای پردازش تصاویر و سیگنال‌های دوبعدی استفاده می‌شود. شبکه عصبی پیچشی قادر است الگوهای خاصی را در تصاویر مانند تشخیص چهره، تشخیص اشیاء، تشخیص اعداد و حروف و ... شناسایی کند. این شبکه‌ها معمولاً در برنامه‌های تشخیص تصویر و تشخیص الگو به کار می‌روند.

- شبکه عصبی بازگشتی

در این شاخه، شبکه‌های عصبی طراحی می‌شوند که قادر به پردازش داده‌های دنباله‌ای هستند .این شبکه‌ها می‌توانند الگوهای زمانی و ترتیبی را در داده‌ها شناسایی کنند .برخی از کاربردهای شبکه عصبی بازگشتی شامل ترجمه ماشینی، تولید متن، تشخیص گفتار و پردازش زبان طبیعی می‌شود.

9-7- یادگیری ماشین

منظور از یادگیری ماشینی، توانایی ماشین‌ها برای یادگیری خودکار از داده‌ها و الگوریتم‌ها است. این بخش به‌عنوان یکی از شاخه‌های سخت هوش مصنوعی شناخته می‌شود. یادگیری ماشینی عملکردها را با استفاده از

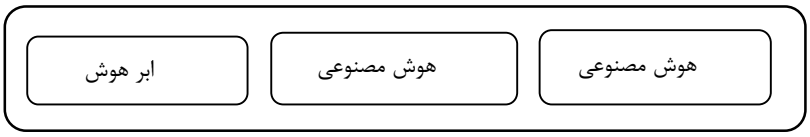
تجربیات گذشته بهبود می‌بخشد و می‌تواند بدون برنامه‌ریزی‌های خاص تصمیم‌گیری کند. این فرآیند با جمع‌آوری داده‌های تاریخی مانند دستورالعمل‌ها آغاز می‌شود تا بتواند مدل‌های منطقی را برای استنتاج آینده بسازد. الگوریتم‌های یادگیری ماشینی به بخش زیر طبقه بندی می‌شوند:

- یادگیری تحت نظارت: ماشین‌ها با داده‌های برچسب‌گذاری شده برای پیش‌بینی نتیجه آموزش داده می‌شوند.
- یادگیری بدون نظارت: ماشین‌ها با داده‌های بدون برچسب آموزش داده می‌شوند و مدل اطلاعات را از ورودی استخراج می‌کنند تا با شناسایی ویژگی‌ها و الگوها یک نتیجه را ایجاد کنند.
- یادگیری تقویتی: ماشین‌ها از طریق آزمون و خطا یاد می‌گیرند و برای شکل دادن به اقدامات از «بازخورد» استفاده می‌کنند الگوریتم‌ها و مدل‌هایی طراحی می‌شوند که قادر به یادگیری از طریق «تجربه و تعامل با محیط» هستند. این الگوریتم‌ها با استفاده از سیگنال‌های تقویت، عملکرد خود را در انجام یک وظیفه خاص بر اساس تجربه در محیط بهبود می‌بخشند. یادگیری تقویتی برای کاربردهایی مانند بازی‌های رایانه‌ای، کنترل ربات‌ها و مدیریت منابع استفاده می‌شود.

7-10- منطق فازی

منطق فازی تکنیکی است که به حل مسائل یا عباراتی که می‌توانند درست یا نادرست باشند کمک می‌کند. این روش با در نظر گرفتن تمام احتمالات موجود بین مقادیر دیجیتالی «بله» و «نه» تصمیمات انسانی را کپی می‌کند. به بیان ساده‌تر میزان درستی یک فرضیه را می‌سنجد. شما می‌توانید از این شاخه از هوش مصنوعی برای استدلال در مورد موضوعات نامشخص استفاده کنید. منطق فازی یک روش راحت و انعطاف‌پذیر برای پیاده‌سازی تکنیک‌های یادگیری ماشینی و کپی کردن منطقی فکر انسان است.

8- سطوح مختلف هوش مصنوعی



شکل 2: سطوح مختلف مصنوعی

8-1-هوش مصنوعی باریک (ANI[1])

[1] Narrow artificial intelligence
2 Natural language processing

هوش مصنوعی ANIکه به آن هوش مصنوعی ضعیف یا هوش مصنوعی باریک نیز گفته می‌شود تنها نوع هوش مصنوعی است که تا به امروز با موفقیت به آن دست یافتیم ANI .هدف گرا است و برای انجام وظایف منحصر به فرد مانند تشخیص چهره، تشخیص گفتار، رانندگی با ماشین یا جستجو در اینترنت طراحی شده و در تکمیل کار خاصی که برای انجام آن برنامه ریزی شده بسیار هوشمند است.

اگرچه این ماشین‌ها ممکن است هوشمند به نظر برسند اما تحت نظر مجموعه کوچکی از محدودیت‌ها کار می‌کنند؛ به همین دلیل است که این نوع معمولاً به‌عنوان هوش مصنوعی ضعیف شناخته می‌شوند ANI .هوش انسانی را تقلید یا تکرار نمی‌کند بلکه صرفاً رفتار انسان را بر اساس طیف محدودی از پارامترها و زمینه‌ها شبیه سازی می‌کند. تشخیص گفتار و زبان دستیار مجازی Siri در آیفون‌ها یا تشخیص دید اتومبیل‌های خودران را در نظر بگیرید که بر اساس سابقه خریدتان محصولاتی را به شما پیشنهاد می‌دهند. این سیستم‌ها فقط تکمیل وظایف خاصی را یاد می‌گیرند.

هوش مصنوعی ANI در دهه گذشته پیشرفت‌های متعددی را تجربه کرد و توسط دستاوردهای یادگیری ماشین و یادگیری عمیق تقویت شد؛ به‌عنوان‌مثال امروزه از سیستم‌های هوش مصنوعی در پزشکی برای تشخیص سرطان و سایر بیماری‌ها از طریق تکرار شناخت و استدلال انسانی استفاده می‌شود ANI از پردازش زبان طبیعی یا NLP[2] برای انجام وظایف گوناگون کمک می‌گیرد NLP در چت‌بات‌ها و فناوری‌های مشابه هوش مصنوعی مشهود است و با درک گفتار و متن به زبان طبیعی با انسان‌ها به شیوه‌ای طبیعی و شخصی شده تعامل می‌کند. نمونه‌هایی از هوش مصنوعی باریک به شرح جدول زیر هستند.

جدول 1: نمونه‌هایی‌های هوش مصنوعی باریک

الگوریتم RankBrain گوگل	نرم افزارهای تشخیص چهره	فیلترهای هرزنامه ایمیل
Siri توسط اپل	ابزارهای نقشه برداری	ابزارهای نظارت بر رسانه‌های اجتماعی
Alexa توسط آمازون	ابزارهای مخصوص پیش بینی بیماری	توصیه محتواهای مختلف به کاربر بر اساس رفتار او
Cortanaتوسط مایکروسافت	تولید و ربات‌های مخصوص پهپاد	

2-8-هوش مصنوعی عمومی (AGI[1])

هوش مصنوعی قوی یا عمیق یک مفهوم ماشینی با هوش عمومی است که هوش یا رفتارهای انسان را تقلید می‌کند و توانایی یادگیری و استفاده از هوش خود را برای حل هر مشکلی دارد AGI می‌تواند به گونه‌ای فکر کند، بفهمد و عمل کند که از انسان در هر موقعیتی قابل تشخیص نیست.

1 General artificial intelligence

محققان و دانشمندان هوش مصنوعی هنوز به AGI دست پیدا نکردند. آن‌ها برای موفقیت در این زمینه باید راهی بیابند تا ماشین‌ها را آگاه کرده و مجموعه‌ای کامل از توانایی‌های شناختی را برنامه ریزی کنند. ماشین‌ها باید توانایی استفاده از دانش تجربی را در طیف وسیع‌تری از مسائل مختلف به دست آورند.

"K computer"که توسط شرکت فوجیتسو و موسسه RIKEN ساخته شده یکی از سریع‌ترین ابررایانه‌ها است K computer بیشترین تلاش برای دستیابی به هوش مصنوعی AGI است اما با توجه به اینکه 40 دقیقه طول کشید تا یک ثانیه فعالیت عصبی شبیه‌سازی شود؛ پس تعیین اینکه آیا هوش مصنوعی قوی خواهد بود یا نه دشوار است.

8-3- ابر هوش مصنوعی (ASI[1])

ابر هوش مصنوعی یا ASI در واقع یک هوش مصنوعی فرضی است که فقط هوش و رفتار انسان را تقلید یا درک نمی‌کند ASI جایی است که ماشین‌ها خودآگاه می‌شوند و از ظرفیت هوش و توانایی انسان فراتر می‌روند. ابر هوش مدت‌هاست که الهام بخش داستان‌های علمی تخیلی دیستوپیایی بوده است. در داستان‌های او ربات‌ها بشریت را زیر پا می‌گذارند، سرنگون می‌کنند یا به بردگی می‌گیرند. ASI از نظر تئوری در هر کاری که انجام می‌دهیم از ریاضیات گرفته تا علوم، ورزش، هنر، پزشکی، سرگرمی‌ها، روابط عاطفی و ... بهتر است ASI حافظه بیشتر و توانایی سریع‌تری برای پردازش و تجزیه و تحلیل داده‌ها و محرک‌ها دارد؛ در نتیجه توانایی تصمیم گیری و حل مسئله آن بسیار برتر از انسان‌ها است. پتانسیل داشتن چنین ماشین‌های قدرتمندی ممکن است جذاب به نظر برسد اما این مفهوم پیامدهای ناشناخته زیادی دارد.

9- کاربردهای هوش مصنوعی

یکی از کاربرد های مهم هوش مصنوعی در صنایع نظامی است بطوریکه استفاده از هوش مصنوعی در صنعت نظامی به طور فزاینده ای با هدف افزایش دقت در صحنه نبرد و رویه های عملیاتی رایج شده است. سیستم های هوش مصنوعی می توانند برای کنترل پهپادها و سایر سیستم های سلاح استفاده شوند و امکان پایش، تجزیه و تحلیل حرکات و تهدیدات دشمن را در زمان واقعی فراهم کنند. علاوه بر این، برای پیش بینی پاسخ های احتمالی دشمن، شناسایی نقاط ضعف و بهینه سازی عملیات نظامی استفاده می شوند (رحمانی، م و علیزاده، ح . 1400)

هوش مصنوعی می‌تواند قابلیت‌های تحرک یگان نظامی را از طریق تشخیص هدف، سیستم های سلاح خودکار، ابزار های حمایتی و برنامه ریزی بهبود بخشد. این فناوری در همه زمینه های نظامی (زمین، دریا، هوا، فضا، اطلاعات) و در تمام سطوح دفاعی(سیاسی، راهبردی، عملیاتی و تاکتیکی) کاربرد دارد. هوش مصنوعی و ارتباط آن با شبکه جهانی اینترنت، هسته اصلی فناوری اطلاعات در بخش دفاعی تلقی می شود. به همین دلیل

[1] Artificial Supper intelligence

موضوعی تحت عنوان حاکمیت هوش مصنوعی مطرح شده است که بر متغیر هایی همانند پویـایی هـای رقابـت نظامی، نابرابری های اجتماعی و اقتصادی، آگاهی های عامه مردم و پایش تمرکز کرده است(perry, 2019) .

کاربرد های نوین هوش مصنوعی از داده کاوی، رباتیک و پردازش زبان طبیعی فراتـر رفتـه و حیطـه هـایی همانند مراقبت نظامی، شناسایی، ارزیابی تهدید، مین گذاری زیر آب، امنیت سایبری، آنالیز هوشمند، فرماندهی و کنترل، و آموزش در بر می گیرد(James, 2018).

امروزه هوش مصنوعی به ابزار قدرت انسان تبدیل شده است و هر کشوری سعی دارد با به‌کارگیری آن در تجهیزات دفاعی و ادوات نظامی خود، در این زمینه پیشرو شده و در صورت هرگونه تهدید، به مقابله با آن بپردازد. برخی از تجهیزات هوشمند به‌کارگرفته‌شده در ظرفیت‌های نظامی عبارتند از: (حسنی، م و همکاران، 1398)

- ربات هوشمند Armored Combat Engineer Robot و ربات‌های Boston Dynamics
- میکرو پهپادهای قاتل MICRO DRONES KILLER
- شبکه‌های هوشمند فرماندهی و کنترل شناختی و هوشمندسازی هواگردهای نسل 5 و 6
- تولید سربازان سایبرگ (نیمی انسان و نیمی ماشین)
- ادوات و تجهیزات و تسهیلات نظامی و سامانه‌های سپر دفاعی و سایبری
- جاسوسان حیوانی (ساخت روبات با ظاهر و ویژگی‌های حیوانات، پرندگان، حشرات و...)
- ساخت سلول‌های هوشمند زیستی برای درگیری بیولوژیک در درون بدن سربازان دشمن
- ماشین‌های رمزنگار و رمزگشایی مخابراتی برای امنیت بخشی به ارتباطات نظامی
- ساخت ماشین‌هایی برای کار در مناطقی که حضور انسان در آنجا پرخطر یا غیرممکن می‌باشد.
- هوشمندسازی ساختار و معماری‌های فرماندهی و کنترل شناختی بر اساس پایه‌ریزی بر اساس هوش مصنوعی

جدول 2- کاربردهای هوش مصنوعی در ابعاد مختلف (غلامی و همکاران، 1395)

مدل‌های هوش مصنوعی با استفاده از الگوریتم‌های یادگیری عمیق قادر به تشخیص اجسام مختلف مانند خودروها، انسان‌ها، حیوانات و اشیاء مختلف هستند و در حوزه‌هایی مانند خودروهای خودران، امنیت و تصویربرداری استفاده می‌شود.	تشخیص اجسام Object Recognition
با استفاده از الگوریتم‌های یادگیری عمیق، مدل‌های هوش مصنوعی قادر به تشخیص و شناسایی افراد مختلف بر اساس ویژگی‌های چهره خواهند بود. در حوزه‌هایی مانند امنیت، تشخیص هویت و سیستم‌های حضور و غیاب به کار می‌رود.	تشخیص چهره Face Recognition
با استفاده از الگوریتم‌های پردازش سیگنال صوتی و یادگیری عمیق قادر به تشخیص کلمات و جملات از طریق گفتار هستند و در حوزه‌هایی مانند سیستم‌های خودکار ترجمه، سیستم‌های شناسایی صدا و خودروهای خودران استفاده می‌شود.	تشخیص گفتار Speech Recognition
هوش مصنوعی در ایجاد دیپ‌فیک‌ها (تصاویر و ویدئوهای تقلبی) و استفاده از شبکه‌های مولد به کار می‌رود و با استفاده از الگوریتم‌های یادگیری عمیق قادر به تولید تصاویر و ویدئوهای واقعی خواهد بود. مانند سینما، تبلیغات و امنیت آن	دیپ‌فیک و شبکه‌های مولد
هوش مصنوعی با کمک الگوریتم‌های یادگیری عمیق و پردازش تصویر و گفتار می‌تواند سیستم‌هایی را طراحی کند که قادر به تشخیص و پاسخ به محیط و وظایف مختلف هستند. رباتیک در حوزه‌های گوناگون قابل استفاده است.	رباتیک و هوش مصنوعی
در تحلیل داده‌ها و پیش‌بینی رویدادها هم نقش دارد و با الگوریتم‌های یادگیری ماشین و تحلیل داده‌ها می‌توان ماشین‌هایی را ساخت که الگوها و روندهای اقتصادی را تشخیص می‌دهند مانند بورس، بازار سرمایه	هوش مصنوعی در اقتصاد
تولید، منابع انسانی، بازاریابی، فروش، زنجیره تأمین و تدارکات، خدمات مشتری، کنترل کیفیت، فناوری اطلاعات، امور مالی و موارد دیگر. از ماشین‌آلات و وسایل نقلیه خودکار تا الگوریتم‌هایی که تقلب مشتری را تشخیص می‌دهند.	هوش مصنوعی در حوزه کسب و کار
هوش مصنوعی به مربیان در انجام وظایف غیر آموزشی مانند تسهیل و خودکارسازی پیام‌های شخصی به دانش‌آموزان، کارهای پشتیبانی مانند درجه‌بندی مدارک، تعاملات با والدین، فرایند ثبت نام	در حوزه آموزش و پرورش
نظارت بر وضعیت ماشین‌های تولید، تعمیر و نگهداری دستگاه‌ها، تجزیه و تحلیل شرایط، بررسی کارایی هر بخش به‌صورت مجزا از قابلیت‌های هوش مصنوعی در حوزه تولید است.	هوش مصنوعی در حوزه تولید
سیستم‌های هوش مصنوعی در زمینه شناسایی و مبارزه با حملات سایبری و سایر تهدیدات سایبری بر اساس ورودی مداوم داده‌ها، شناسایی الگوها و عقب‌نشینی حملات قابل استفاده خواهد بود.	هوش مصنوعی در برقراری امنیت
هوشمندسازی محصولات و خدمات، فرآیندها از طریق تجزیه و تحلیل داده‌ها، تعامل با مشتریان و کارمندان	تجارت الکترونیک
هوش مصنوعی این قابلیت را دارد تا تغییر در الگوی تراکنش‌ها را که نشانه کلاهبرداری است را تشخیص دهد؛ همچنین می‌تواند خطرات وام را بهتر پیش بینی و ارزیابی کند .	بانکداری و بازارهای مالی
آزمایش و اجرای الگوریتم‌های هوشمند در شاخه‌های گوناگون مراقبت‌های پزشکی هستند .کاربرد این الگوریتم‌ها، از پیشگیری و غربالگری گرفته تا تشخیص، درمان و کنترل بیماری‌ها، گسترده است.	هوش مصنوعی در پزشکی

ستاره شناسان برای ایجاد ابزارهای جدید به یادگیری ماشین و هوش مصنوعی روی آورند.	در اکتشافات فضایی

10- امنیت اطلاعات هوش مصنوعی با سیستم‌های رمزنگاری

با درنظرگرفتن امنیت، می‌توان اطمینان حاصل کرد که سیستم‌های هوش مصنوعی ایمن هستند و نمی‌توانند برای آسیب رساندن به فرایندها یا زیرساخت¬ها استفاده شوند. توجه به این نکته مهم است که هیچ مدل تصمیم‌گیری کاملی وجود ندارد. هر مدل تصمیم‌گیری دارای نقاط قوت و ضعف خاص خود است. مهم است مدلی را انتخاب کنید که برای نیازهای خاص شما مناسب باشد. در مورد این مسئله، مهم بود مدلی را انتخاب کنیم که بتواند معیارهای مهم را در نظر بگیرد. همچنین مهم است که مدلی را انتخاب کنیم که توسط کارکنان پذیرفته شود. با استفاده از تکنیک تصمیم‌گیری چندمعیاره، می‌توانید اطمینان حاصل کنید که گزینه‌ای را انتخاب می‌کنید که بیشترین اثربخشی را در فرایندهای هوش مصنوعی داشته باشد.

میزان امنیت یک سیستم رمزنگاری به توابع به کاررفته برای رمزکردن و باز نمودن رمز و نیز به اندازۀ کلید مورد استفاده برای این منظور بستگی دارد. مسلماً دستیابی شخص مهاجم به یک کلید بزرگتر سخت‌تر می‌باشد و در واقع به ازای هر بیت افزایش طول کلید، زمان لازم برای جستجوی کامل[1] فضای کلید دو برابر می‌گردد.

سیستم‌های رمزنگاری را می‌توان به دو دستۀ کلی کلید- خصوصی[2] و کلید- عمومی[3] تقسیم نمود. در سیستم‌های کلید- خصوصی از یک کلید برای رمزکردن و باز کردن پیغام استفاده می‌گردد $(k_e = k_d)$. در صورتیکه در سیستم‌های کلید- عمومی دو کلید متفاوت برای انجام این دو فرآیند مورد استفاده قرار می‌گیرند $(k_e \neq k_d)$ (FIPS, 2022).

10-1- سیستم رمز کلید عمومی

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند. (میراکبری، 1403).

این بخش طرح جدید را توضیح می دهد. ابتدا به تئوری مفیدی نگاه می کنیم

[1] Exhaustive Search
[2] - Private Key
[3] - Public Key

تئوری 2-1: اگر $A=(a_{ij})$ یک ماتریس n بعدی باشد و $N=pq$ تولید شده از دو عدد اولیه p و q باشد. $A=\mathrm{mod}N$ در صورتی که فقط هر دوی $A=\mathrm{mod}\,p$ و $A=\mathrm{mod}\,q$ معکوس پذیر باشند، معکوس پذیر خواهد بود. فرض کنیم k پارامتر امنیت و n بعد ماتریسهای مورد استفاده در طول رمز کردن و رمزگشایی باشند آنگاه الگوریتم از سه زیر الگوریتم تشکیل شده که شامل تولید کلید و رمزنگاری و رمز گشایی می باشد (Kalesth,2022).

- **تولید کلید**

الگوریتم تولید کلید بر مبنای مراحل زیر انجام می گیرد:

الف) بصورت تصادفی دو عدد اولیه بزرگ p و q را که p دارای k بیت و q دارای $3k$ بیت است را انتخاب کرده که براحتی می تواند با استفاده از الگوریتم های تولید اعداد اولیه بزرگ انجام گیرد. حال $N=pq$ قرار می دهیم.

ب). m,e,b اعداد صحیح تصادفی هستند که تقریباً طبق روابط زیرند که m باند بالایی برای بلوک های متن اصلی و e باند بالایی برای بردار خطا هستند.

(1) $\quad e\approx q^{0.3} \qquad b\approx q^{0.1}\; m\approx q^{0.5}$

ج) بصورت تصادفی یک ماتریس کوچک n بعدی در مد q معکوس پذیر $B=(bij)$ را با استفاده از الگوریتم 2-1 انتخاب می کنیم که بعداً این الگوریتم آورده خواهد شد. همچنین bijها باید شرط زیر را بر آورده کنند که

(2)

$$\left|b_{ij}\right|<b$$

د) صورت تصادفی n عدد صحیح a_i را انتخاب کرده که $i=1,2.....n$ بطوریکه

$$q^{0.4}<a_i<q^{0.5} \qquad (3)$$

و همچنین معکوس آن را محاسبه کرده که $u_i \bmod q$ است. $A=diag(a_1.....a_n)$ و همچنین $U=diag(u_1.....u_n)$. مقدار زیر را نیز محاسبه می کنیم.

(4)

$$G=UB=A^{-1}B(\mathrm{mod}\,q)$$

و) بصورت تصادفی یک ماتریس معکوس پذیر n بعدی در مد p را با نام $T=(t_{ij})$ انتخاب کرده که در آن از الگوریتم 2-1 استفاده می شود. تئوری 2-1 به ما می گوید که ماتریس معکوس پذیر H در مد N که $H=(h_{ij})$ بوسیله مساله باقیمانده چینی ساخته می شود. یعنی:

$$h_{ij} = g_{ij} \bmod q \quad (5)$$

$$h_{ij} = t_{ij} \bmod p \quad (6)$$

ماتریس چهار گانه (H, N, m, e) کلید عمومی را تشکیل می دهد. و کلید خصوصی شامل q و $a_1,\ldots,a_n$ است.

الگوریتم 2-1 برای پیدا کردن یک ماتریس n بعدی در مد q که معکوس پذیر باشد با نام $B = (b_{ij})$ و $T = (t_{ij})$ (که ماتریس معکوس پذیر در مد p است بکار می رود.

الگوریتم 2-1

الف) بصورت تصادفی یک رشته غیر صفر $b_i = b_{11}.....,b_{1n}$ تولید می‌کنیم.

ب) برای $i = 2,.....,n-1$ بصورت تصادفی یک بردار غیر صفر $b_i = b_{i1}.....,b_{in}$ تولید می کنیم.

ج) با استفاده از روش حذف گاوسی مشخص کرده که آیا bi $b_1....$ بصورت خطی مستقلند یا خیر. اگر جواب بله است bi را ذخیره کنید و $i=i+1$ را قرار داده و به مرحله (ب) می رویم. در غیر این صورت bi را دور ریخته و بصورت تصادفی یک رشته برداری غیر صفر bi دیگر تولید کرده و به مرحله بعد می‌رویم.

د) بصورت تصادفی یک بردار غیر صفر $bn=(b_{n1}, . b_{nn})$ تولید کرده و. مقدار $det(B)(mod\ q)$ را برای ماتریس B محاسبه می کنیم و با استفاده از روش حذف گاوسی مشخص کرده که آیا این مقدار محاسبه شده برابر با صفر است یا معادل با آن آیا $gcd(det(B),q)=1$ است. اگر بله $B=(bij)$ خروجی الگوریتم است و از الگوریتم خارج شده. در غیر اینصورت به مرحله(د) می رویم (Youssef,2023).

- **رمزنگاری**

ابتدا بصورت تصادفی یک بردار ماتریس n بعدی $E_i = (e_1.....,e_n)^T$ ایجاد کرده که اندازه ei ها از e انتخاب شده در بند (ب) بالا کمتر باشد. رشته متن اصلی M که به n بلوکهایی به شکل M=(m1, . . . , mn)T می شکند که هر بلوک باید $mi<m$ باشد که در بند (ب) بالا بدست آمده است. حال بصورت زیر رمز می کنیم.

(7)

$$C = (c_1,....., c_n)^T = M + HE(\bmod n)$$

- **رمزگشایی**

برای رمزگشایی یک متن رمز شده مشخص C مراحل طبق زیر است:

$$D = (d_1, \ldots, d_n)^T = C = M + GE(mod\ q) \quad \textbf{(8)}$$

$$S=(s_1, \ldots, s_n)T = AD = AM + AGE = AM + BE(mod\ q) \quad \textbf{(9)}$$

که داریم:

$$m_i = \frac{s_i - < s_i >_{a_i}}{a_i} \quad , \quad i = 1,\dots, n \tag{10}$$

که $<b>_a$ اشاره دارد به باقیمانده ای با کمترین اندازه از b mod a در اینجا به این قضیه اشاره می شود که آیا ماتریس H معکوس پذیر درمد N است یا خیر در رمزگشایی تاثیری ندارد. به هر حال اگر ما یک ماتریس H غیر معکوس پذیر در مد N انتخاب کنیم و یا بطور معادل $gcd(det(H),N)>1$ در اینصورت امنیت سیستم ما کاهش خواهد یافت. این بخاطر آنست که $gcd(det(H),N)\sim=N$ و فاکتور مناسبی از N قابل مشاهده است.

مشاهده می شودکه کارایی روش دارای سرعت بالایی است.زیرا در کل بازه رمزنگاری و رمزگشایی بترتیب تنها $n2$ بار در مد N عمل ضرب انجام می گیرد و n^2 بار در مد q عمل ضرب داریم. بنابراین پیچیدگی محاسباتی برای رمزنگاری و رمز گشایی برابر با $O(n^2k^2)$ است. بسط متن رمز شده در سیستم ما که با نسبت طول بیت متن رمز شده به طول بیت متن اصلی است بصورت زیر تخمین زده می شود(Bellare, 2022).

$$f \approx \frac{n \log_2 N}{n \log_2 m} \approx \frac{4\ nk}{1.5\ nk} = \frac{8}{3} \tag{11}$$

10-2- آنالیز امنیت

در رمزنگاری با کلید عمومی دو روش برای آنالیز امنیت بکار می رود. یکی تئوری امنیت قابل اثبات است که برای کاهش امنیت PKC ها تحت بعضی از مدلی های حمله برای مسائل سخت ریاضی است. روش دیگر تحویل PKC به متن برای حمله است. اگر PKC در برابر همه حملات شناخته شده امن باشد(Diffie, 2024) .

- فاکتورگیری از N

فرض کنید که ما یک دشمن بنام Eve داریم که تلاش می کند سیستم را تسلیم کند، تلاش برای این است که ابتدا فاکتور مدول N=pq پیدا شده و سپس جستجو برای ماتریس قطری A انجام گیرد. دقت شود که الگوریتم فاکتورگیری کلی بهترین روش NFS[1] به اندازه مدول N بستگی دارد. که این کار غیر ممکن به نظرمی رسد که فاکتور عدد صحیح 1024 بیتی بکار رفته در سیستم ما بوسیله NFS قابل شکسته شدن باشد. برای بهبود امنیت ، ما باید از اعداد اولیه بزرگ برای جلوگیری از جمله بر اساس این الگوریتم فاکتور گیری استفاده می شود.

- حمله تخمین معادلات با اعداد طبیعی همزمان

[1] number field sieve method

در این بخش ما نشان خواهیم داد که جستجو برا ی ماتریس قطری A که رابطه 3 را ارضا می کند معادل حل مساله تئوری عددی سخت است، بطور مثال مساله تخمن معادلات با اعداد طبیعی همزمان که در زیر توضیح داده شده است.

تعریف (مساله تخمین معادلات با اعداد طبیعی همزمان): $n+1$ عدد گویا انتخاب شده اند که $r_1, \ldots$ r_n , $\varepsilon>0$, و یک عدد صحیح $Q>0$ ، پیدا کنید اعداد $p1, \ldots, pn$ و q بطوریکه $0<q<=Q$ و

$$\left| r_i - \frac{p_i}{q} \right| \le \frac{\varepsilon}{q} \quad , \quad i = 1,..., n \tag{12}$$

به عبارت دیگر پیدا کردن n قسمت کسری pi/q ها برای تخمین n عدد ri آنها. محدودیت در n عدد کسری pi/q ها اینست که آنها همه دارای مخرج q یکسان کوچکی هستند و یک صورت کسر کوچک.

3-10- آنالیزحمله و شکستن

که Eve یک ai از کلید عمومی را پیدا کرده به صورتی که Eve با دانستن q می تواند ماتریس G را تنها بوسیله انجام مد q در ماتریس A بدست آورد که به معنای تعیین کردن ai که $q^{0.4} < a_i < q^{0.5}$ و $i=1,\ldots.. n$ بطوریکه $abc(a_i g_{ij} \bmod q)$ که Eve بطور کامل برای ai ها جستجو می‌کند زیرا ai ها مقادیری بین $q^{0.4} < a_i < q^{0.5}$. می گیرند. Eve می تواند ازکلید عمومی (H,N,m,e) ماتریس‌های $o=diag(oi)$ و $p=(pij)$ را طبق زیر بدست آورد:

۱. $o = diag(o_1,\ldots\ldots o_n)$ و $\alpha<oi<\beta$ و $i=1,\ldots\ldots. n$ بطوریکه α و β بترتیب باند بالا و پایین α هستند.

۲. $\left| p_{ij} \right| < \gamma, \ \ i, j = 1,..., n$

۳. $H = O^{-1} P (\bmod N)$

۴. $-a/2 < ne\gamma < a/2$ و $0 < m\alpha + ne\gamma < m\beta + ne\gamma < N$

اگر چنین ماتریس های O و P ای یافت شوند، Eve می تواند رمزگشایی کند هر متن رمز شده C را با استفاده از O و P . بطوریکه

$$W=(Iw1, \ldots, wn)T = OC=O(M+HE)=OM+PE(mod\ N) \tag{13}$$

حال Eve پیام mi را بصورت زیر رمزگشایی می کند.

$$m_i = \frac{w_i - < w_i >_{o_i}}{o_i} \quad , i = 1,2,....n \tag{14}$$

همانطور که بحث شد در معرفی، امنیت سیستم ما بر مبنای دو مساله تئوری عددی خود سر انجام می گیرد، که مساله فاکتور گیری و مساله تخمین معادلات با اعداد طبیعی بطور همزمان است. برای شکستن سیستم ما بطور کلی، *Eve* باید از مدول N فاکتور گرفته و سپس مساله تخمین معادلات با اعداد طبیعی همزمان را حل کند.

یک مقایسه بین این سیستم در مقاله با روش *RSA* و *El Gamal* در جدول زیر نشان داده شده است.

جدول 4- مقایسه امنیت در سیستم کلید عمومی با روشهای رمزنگاری

	پیچیدگی رمزنگاری	پیچیدگی رمزگشایی	بسط متن رمز شده
این سیستم	$O(n^2k^2)$	$O(n^2k^2)$	8:3
RSA	$O(k^3)$	$O(k^3)$	1:1
El Gamal	$O(k^3)$	$O(k^3)$	2:1

برای اثبات سرعت سریع سیستم ما در زیر یک مثال ذکر می شود:

فرض کنید که ما $k=256$ و $n=16$ انتخاب کنیم، طول مدول N بکار رفته در سیستم ما 1024 بیت خواهد بود. ما همچنین فرض می کنیم که *RSA* نیز از ماژول 1024 استفاده می کند. اگر سیستم پیشنهادی برای رمز کردن پیام بکار رود، رمزنگاری تقریباً به اندازه *162*10242* عمل و رمزگشایی *162*7682* عمل را می گیرد . در مقایسه *RSA* در حدود *10243* عمل را در رمزگشایی و رمزنگاری انجام می دهد. پس سیستم ما دارای رمزنگاری سه مرتبه سریعتر از *RSA* و 6 مرتبه سریعتر از *RSA* در رمزگشایی است.

11- نتیجه‌گیری

در دیدگاه راهبرد نظامی به حوزه هوش مصنوعی باید این نکته را متذکر شویم که در مأموریت‌های محوله نظامی و در تمامی مراحل و گام‌ها می‌توان از عنصر ماشین و در نهایت امر هوش مصنوعی برای هدایت و کنترل این ماشین بهره برد؛ ولی امر تصمیم‌گیری توسط عامل انسانی (در گام آخر) انجام خواهد پذیرفت. همان گونه که در تجربه‌های شکست‌خورده ارتش‌های بزرگ دیده شده است، نمی‌توان تمامی امور را به ماشین و هوش مصنوعی سپرد. تنها با به‌کارگیری این ظرفیت می‌توان قدرت و سرعت واکنش‌های پدافندی و در نگاه کلی تصمیم‌گیری و کیفیت آن را ارتقا بخشید. زیرا هوش مصنوعی همان گونه که از نامش پیداست در خور مصنوعات و ماشین است و تصمیم‌ساز و برتری سازند و نه تصمیم‌گیر.

ظهور این پدیده در سامانه‌های پدافندی به‌خصوص در سامانه‌های بومی بسیار لازم و مبرهن است. خیزش به این نگاه که سامانه‌ها و در غایت امر فرماندهی و کنترل شناختی باید با سرعت‌ها و ظرفیت‌های امروزی مرتبط و متناسب گردد می‌تواند سرعت عمل و دقت در تصمیم‌گیری در فرماندهان را در پی داشته باشد. از طرفی حفظ جان عامل انسانی یکی از اولویت‌های خدشه‌ناپذیر جنگ‌های آینده است. جنگ‌های آینده در بستر

شبکه‌ها و ارتباطات داده‌ای رخ‌داده می‌شود و به قول یکی از نظریه‌پردازان بیشتر از این که جنگ‌های آینده بر سر آب باشد بر سر داده خواهد بود و ظهور پدیده‌های اطلاعاتی از جمله عظیم‌داده‌ها و محاسبات ابری از این منظر برای فعالیت‌های نظامی قابل‌اهمیت است که در فواصل زیاد، سرعت‌های بالا، پنهان‌کاری‌های حداکثری و... تنها راه نجات قابل‌تصور هوش مصنوعی و به‌کاربردن این ظرفیت در سامانه‌های نظامی است.

آموزش کارکنان در مورد امنیت هوش مصنوعی: کارکنان باید در مورد خطرات امنیت هوش مصنوعی و نحوه محافظت از خود در برابر این خطرات آموزش ببینند. این شامل آموزش در مورد انواع حملات امنیتی، نحوه شناسایی حملات و نحوه گزارش حملات است. ایجاد یک برنامه امنیت هوش مصنوعی: یک برنامه امنیت هوش مصنوعی باید برای شناسایی، ارزیابی و کاهش خطرات امنیتی هوش مصنوعی ایجاد شود. این برنامه باید شامل اقداماتی مانند آموزش کارکنان، استفاده از سیستم‌های ایمن و نظارت بر استفاده از هوش مصنوعی باشد.

برقراری ارتباطات در هوش مصنوعی به صورت ذاتی ناامن هستند و نیازمند یک وظایف مدیریتی امنیتی مقاوم‌اند تا آسیب‌پذیری‌های این گونه اطلاعات را در هوش مصنوعی پوشش دهد (میراکبری، 1401).

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، ردوبدل می‌شده، استفاده شده است تا پیغامهای آنها محرمانه بماند. هنگامی که با امنیت اطلاعات در فضای سایبر سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

پردازنده‌های رمزنگاری، راهکاری جهت دستیابی به نقاط قوت سخت‌افزارهای خاصِ رمزنگاری (ASIC) و پردازنده‌های همه‌منظوره می‌باشند؛ بدین صورت که هم دارای قابلیت انعطاف زیاد (همانند پردازنده‌های همه‌منظوره) بوده و هم دارای سرعت اجرای بالا (بیشتر از پردازنده‌های همه‌منظوره و نزدیک به سخت‌افزارهای خاص) می‌باشند. بنابراین پیاده‌سازی بهینه و سریع هر یک از این اجزاء عملیاتی در پردازنده‌های هوش مصنوعی می‌تواند اثر قابل ملاحظه‌ای در افزایش کارآیی و سرعت اجرای الگوریتم‌های هوش مصنوعی در صحنه نبرد داشته باشد. در این پردازنده هدف اصلی، بهینه‌سازی معماری پردازنده، برای دستیابی به سرعت‌های رمزنگاری بالا بوده است؛ ولیکن در کاربردهای بسیاری، توان مصرفی پائین در اولویت می‌باشد. برای استفاده از پردازندهٔ رمزنگار در این کاربردها، نیاز می‌باشد تا در معماری پردازنده و همچنین ریزواحدهای آن تجدید نظر شده و یا حتی از ابتدا اقدام به طراحی مجدد پردازنده با هدف کاهش توان مصرفی (حتی به قیمت کاهش سرعت) نمائیم. از دیگر نیازهای پردازنده‌های رمزنگار، مقاومت در برابر حملات کانال جانبی می‌باشد. این نیاز معمولاً در پردازنده‌های کم مصرفی که در ابزارهای قابل‌حمل پیاده‌سازی می‌گردند، بیشتر احساس می‌گردد. طراحی یک پردازندهٔ رمزنگار، با هدف افزایش مقاومت در برابر حملات کانال جانبی، می‌تواند یکی دیگر از زمینه‌های فعالیت‌های آینده در صحنه نبرد باشد.

12- پیشنهادات

برای دفاع از کشور و تأمین اهداف و منافع ملی بایستی راهبردی متوازن با اهداف و توانمندی‌ها و عناصر و مؤلفه‌های قدرت نظامی اتخاذ نمود. با عنایت به نتایج به دست آمده از این تحقیق، امید است فرماندهان و طراحان عملیات در نیروهای مسلح در راستای افزایش کارایی و اثربخشی و با بکارگیری پیشنهادهای ذیل گامی در راستای پیشبرد اهداف سازمان بردارند.

- مفاهیم و عوامل اجرای هوش مصنوعی در آیین‌نامه‌ها و متون آموزشی لحاظ گردد.
- نتایج و مولفه‌های شناخته شده در این تحقیق در سیستم‌های مدیریتی و فرماندهی مورد استفاده قرار گیرد.
- به هوش مصنوعی در سازمان های نظامی پرداخته شود و معیارها و پارامترهای آن استخراج گردد.

برای استفاده ایمن از هوش مصنوعی در سازمان های نظامی موارد زیر لحاظ گردد:

- سرمایه‌گذاری در تحقیق و توسعه هوش مصنوعی.
- آموزش کارکنان در مورد هوش مصنوعی.
- توسعه استانداردهای اخلاقی برای استفاده از هوش مصنوعی.
- نظارت بر عملکرد هوش مصنوعی.
- ارتقای شفافیت در مورد نحوه استفاده از هوش مصنوعی.

13- منابع

رحمانی، م و علیزاده، ح . (1400). کاربردهای فناوری هوش مصنوعی در سامانه‌های فرماندهی و کنترل شناختی هوشمند، منتشر شده در دو فصل نامه علمی بازی جنگ، ص 70-101 .

عظیم‌زاده، ح و همکاران (1401). کاربست هوش مصنوعی برای پشتیبانی تصمیم در سیستم‌های فرماندهی و کنترل شناختی، ارائه شده در اولین کنفرانس بین‌المللی فرماندهی و کنترل شناختی. منتشر شده در وب‌سایت همایش

میراکبری، سید روح اله (1403)، "مدیریت و فرماندهی در سازمان با فناوری اطلاعات و افزایش امنیت آن" دومین همایش ملی فرماندهی و مدیریت در جنگ‌های آینده با رویکرد شناختی، تهران: دانشگاه افسری امام علی(ع).

میراکبری، سید روح اله (1401)، " نقش علم و فناوری، ارتباطات نظامی در فرماندهی و کنترل جنگ‌های آینده " همایش ملی جایگاه علم و فناوری در دفاع مقدس, دانشگاه دفاع عالی ملی.

میراکبری، سید روح اله (1402)، " مدیریت و فرماندهی در سازمان با فناوری اطلاعات و افزایش امنیت آن" اولین همایش ملی فرماندهی و مدیریت در جنگ های آینده، دانشگاه افسری امام علی(ع)

حسنی، م.، و همکاران. (1398). کاربرد هوش مصنوعی در فرماندهی و کنترل شناختی. مجله مطالعات راهبردی دفاعی، 26(1)، 131-148.

سید حسینی، م.، و همکاران. (1397). هوش مصنوعی در فرماندهی و کنترل شناختی: چالش‌ها و راهکارها. مجله مطالعات راهبردی دفاعی، 25(1)، 149-166.

غلامی، محمدرضا؛ فرهنگ، ابوالقاسم و حسینی، مریم، 1395، هوش مصنوعی و کاربردهای آن در آموزش، سومین کنفرانس روان‌شناسی و علوم تربیتی، چهارم شهریورماه 1395، مشهد، ایران.

Billing, D. C., Fordy, G. R., Friedl, K. E., & Hasselstrøm, H. (2021). The implications of emerging technology on military human performance research priorities. Journal of Science and Medicine in Sport, 24(10), 947–953.

Perry, W. J. (2019). Technology and national security: risks and responsibilities. Conference on Risk and Responsibility in Contemporary Engineering and Science: French and US Perspectives, France-Stanford Center for Interdisciplinary Sciences, 2.

James, A. D. (2018). Emerging technologies and military capability. Springer.

Krelina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology, 8(1), 24.

FIPS (2022), Federal Information Processing Standards, Publication 46-2, “Data Encryption Standard (DES).

Singer, P. W., & Friedman, A. (2014). Autonomous weapons: An emerging arms race. New York, NY: Oxford University Press.

W. Diffie and M. E. Hellman. (2024), “New directions in Cryptography” IEEE Transactions on Information Theory

Lind, J. D. (2018). The future of command and control: How artificial intelligence will transform the military. New York, NY: Oxford University Press.

Rue L. Byars (2018), Management: Skills and Applications Chicago: Irwin press.18- Karl Kalesth (2022), Knowledge Management from a Business Requires Strategy perspective, Jurnal of FID Review.

Bellare, M, Desai(2022), Relations among notions of security for public-key encryption schemes, Proc. Advances in Cryptology, Crypto’98, California, Santa Barbara.

A.M. Youssef (2023), Cryptanalysis of a public key cryptosystem based on two cryptographic assumptions, The Institution of Engineering and Technology.