شناخت مفاهیم و شاخه‌های کلیدی هوش مصنوعی: مبانی، کاربردها و چشم‌اندازها

مهندس توحید احمدی فر[۱]

حسین مالیمر[۲]

چکیده :

مقاله حاضر به معرفی و بررسی مفاهیم اصلی هوش مصنوعی و شاخه‌های مختلف آن می‌پردازد. ابتدا با مرور تعاریف گوناگون، گستره و اهمیت هوش مصنوعی در شبیه‌سازی تفکر و رفتار انسانی تبیین می‌شود. سپس مهم‌ترین شاخه‌های این حوزه شامل یادگیری ماشین، شبکه‌های عصبی، بینایی ماشین، سامانه‌های خبره، پردازش زبان طبیعی و الگوریتم ژنتیک به تفصیل تشریح می‌شوند. هر شاخه با بیان کاربردها و مثال‌های عملی، نقش خود را در پیشرفت علوم کامپیوتر و صنعت روشن می‌سازد. علاوه بر این، کاربرد هوش مصنوعی در صنایع و همچنین اهمیت تحصیل این رشته در مقاطع عالی مورد توجه قرار گرفته است. متن با تکیه بر منابع علمی، تصویری کلی نگر و جامع از جایگاه فعلی و چشم‌اندازهای آینده هوش مصنوعی ارائه می‌دهد.

کلمات کلیدی: هوش مصنوعی، یادگیری ماشین، شبکه عصبی، امنیت سایبری، پردازش زبان طبیعی

[۱] **استاد دانشگاه و مدیر دفتر توسعه مدیریت شرکت توزیع نیروی برق همدان:**
Eng12ahmadi@gmail.com

[۲] **دانشجوی دانشگاه حاج حشمت شهبازی**

مقدمه

هوش مصنوعی از جمله عرصه‌های نوین و پرشتاب دنیای فناوری است که در دهه‌های اخیر تحولات شگرفی را در زندگی بشر ایجاد کرده است. این حوزه با هدف شبیه‌سازی تفکر، یادگیری و تصمیم‌گیری انسانی در ماشین‌ها و سیستم‌های رایانه‌ای، به سرعت گسترش یافته و زمینه‌های متعددی از جمله علوم کامپیوتر، مهندسی، پزشکی، اقتصاد و صنعت را متحول ساخته است. اهمیت روزافزون هوش مصنوعی باعث شده است که پژوهشگران و دانشگاه‌ها به بررسی عمیق شاخه‌ها و کاربردهای آن بپردازند و شرکت‌های بزرگ جهانی سرمایه‌گذاری گسترده‌ای در این حوزه انجام دهند. شناخت مبانی، شاخه‌ها و کاربردهای هوش مصنوعی، نقطه آغاز ورود به این دنیای پیچیده و پویا است و می‌تواند نقشی کلیدی در توسعه علمی و عملی کشورها ایفا کند.

هوش مصنوعی چیست؟

هوش مصنوعی نه تنها برای درک موجودات هوشمندی می کوشد، بلکه قصد دارد موجودات هوشمند نیز بسازد (تاولی و لورنز، ۲۰۱۹)

با توجه به نظرات محققان و پژوهشگران حوزه هوش مصنوعی، با نگاه تخصصی که به رشته هوش مصنوعی بنگریم، متوجه این موضوع خواهیم شد که تاکنون تعریف روشن و دقیقی از هوش مصنوعی وجود ندارد زیرا که رشته هوش مصنوعی بسیار وسیع و گسترده است. (روتمن، ۲۰۲) اما با توجه به همه تعاریف که در مورد هوش مصنوعی وجود دارد، در چهار تعریف خلاصه می‌شود که عبارتند از:

- سیستم‌هایی که به‌طور منطقی فکر می‌کنند.
- سیستم‌هایی که به‌طور منطقی عمل می‌کنند.
- سیستم‌هایی که مانند انسان فکر می‌کنند.
- سیستم‌هایی که مانند انسان عمل می‌کنند.

هوش ماشینی همان هوش مصنوعی است که دارای ویژگی‌های شبیه به مغز و هوش انسان دارد؛ هوش مصنوعی به سیستم‌های پیچیده‌ای گفته می‌شود که در زمینه‌هایی همچون تفکر، روش‌های استدلال، توانایی یادگیری، حل مسئله و ... رفتار و واکنش‌های شبیه به انسان دارد. رشته هوش مصنوعی در دانشگاه به عنوان یکی از گرایش‌های علوم و مهندسی کامپیوتر به حساب می‌آید که با استفاده از هوش انسانی، توانایی ساخت

سیستم‌های پیچیده را دارد. هوش مصنوعی با تقلید از الگوهای هوش طبیعی انسان، می‌تواند ماشینی با توانایی فکر کردن شبیه به انسان بسازد. (بورکوف، ۲۰۱۹)

کتاب‌هایی در زمینه هوش مصنوعی با دیدی متفاوت به این علم نگاه می‌کنند، تعریفی متفاوت از هوش مصنوعی به این گونه است که هر سیستم و دستگاهی که قابلیت درک محیط اطراف خود را دارد و می‌تواند با محیط اطراف خود بصورت موفیقت‌آمیز ارتباط داشته باشد را به نوعی هوش مصنوعی می‌گویند. تعریف جان مک کارتی بدین شکل است که هوش مصنوعی یعنی علم مهندسی ساخت ماشین‌های هوشمند. (تاولی و لورنز، ۲۰۱۹)

رشته هوش مصنوعی به علومی می‌پردازد که در حوزه‌ی کامپیوتر به دنبال تشخیص، استدلال، درک و عمل هستند. تمامی این موارد که رفتار و واکنش‌های انسانی دیده می‌شود، به یک سیستم کامپیوتری، ربات، ماشین و غیره داده شود به عنوان یک هوش مصنوعی در نظر گرفته می‌شود. رشته هوش مصنوعی با تمامی حوزه‌ها همچون تحلیل داده در ارتباط است؛ رشته هوش مصنوعی مجموعه‌ای از تکنیک‌ها همچون بینایی، پردازش زبان طبیعی، رباتیک، سیستم‌های هوشمند و غیره می‌باشد که در گستره‌ی علم هوش مصنوعی به چندین شاخه تقسیم می‌شوند. (بورکوف، ۲۰۱۹) رشته هوش مصنوعی دارای چندین شاخه است که عبارتند از:

- یادگیری ماشین[۱]
- شبکه عصبی[۲]
- بینایی ماشین[۳]
- سامانه های خبره[۴]
- پردازش زبان طبیعی[۵]
- الگوریتم ژنتیک[۶]
- روباتیک[۷]

[۱] Machine Learning
[۲] Neural Networks
[۳] Machine Vision
[۴] Expert System
[۵] Natural Language Processing
[۶] Genetic Algorithm
[۷] Robotic

هر کدام از این شاخه‌ها در رشته هوش مصنوعی، دنیایی متفاوت از هوش مصنوعی را به ما نشان می‌دهند. یکی از اتفاقات جالب درمورد هوش مصنوعی این است که بسیاری از مردم، یادگیری ماشین (ماشین لرنینگ) را همان هوش مصنوعی می‌دانند، در صورتیکه یادگیری ماشین یکی از شاخه‌های رشته هوش مصنوعی به حساب می‌آید. در مورد هوش مصنوعی و کاربردهای آن می‌توانید مقاله زیر را بصورت تکمیلی مطالعه کنید تا شناختتان نسبت به رشته هوش مصنوعی بیشتر و بهتر شود. (تاولی و لورنز، ۲۰۱۹)

یادگیری ماشین – Machine Learning

یادگیری ماشین یا به اصطلاح ماشین لرنینگ (ML)، یکی از شاخه های هوش مصنوعی است که به شدت طرفدار دارد. بطور خلاصه یادگیری ماشین یعنی هوشمندسازی ماشین بدون اینکه بصورت مستقیم به آن یاد داد؛ بدین صورت ماشین با استفاده از داده‌های ورودی و دستوراتی که به آن داده شده است، فرایند یادگیری را شروع کرده و به مرور زمان ضریب خطا را کم‌تر می‌کند. این یادگیری با استفاده از الگوریتم هایی که شبیه به فرایند ذهن انسان است انجام می‌شود و به مرور زمان دقت آن افزایش پیدا می‌کند که این موضوع بستگی دارد به نوع یادگیری که ماشین انجام می‌دهد، بطور کلی یادگیری ماشین ۳ زیر بخش دارد: (روتمن، ۲۰۲)

- یادگیری با نظارت[۱]
- یادگیری بی نظارت[۲]
- یادگیری تقویتی[۳]

در بخش یادگیری با نظارت، متخصصین با استفاده از اطلاعاتی که بصورت منظم و برچسب‌گذاری شده در اختیار سیستم قرار می‌دهند تا سیستم این اطلاعات را بررسی کند و فرایند خروجی را انجام دهد، بطور مثال لیست پیامک‌های یک سیمکارت را با برچسب ارسال‌کننده در اختیار یک سیستم قرار می‌دهند تا سیستم پیامک‌های تبلیغاتی، خدماتی و شخصی را از یکدیگر جدا کند. (بورکوف، ۲۰۱۹)

در بخش یادگیری بی نظارت، تمامی اطلاعات بدون نظارت و برچسب‌گذاری نشده در اختیار سیستم قرار می‌گیرد تا این اطلاعات توسط سیستم انجام شد، بطور مثال لیستی

---

[۱] Supervised Learning
[۲] Unsupervised Learning
[۳] Reinforcement Learning

از ایمیل‌ها، تماس‌ها و پیامک‌ها را بدون برچسب‌گذاری در اختیار سیستم قرار می‌دهند تا در مرحله اول از یکدیگر جدا شوند و در مرحله دوم موارد اسپم از آن‌ها حذف شود. هرچه این فرایند بیشتر انجام شود، دقت سیستم بالاتر می‌رود. (تاولی و لورنز، ۲۰۱۹)

در بخش یادگیری تقویتی[۱] که یکی از بهترین شاخه های یادگیری ماشین است، تمامی فرایند یادگیری بر اساس تنبیه و تشویق شکل می‌گیرد. از این مدل یادگیری در صنایعی همچون ربات‌ها، مکاترونیک و بازوهای مکانیکی استفاده می‌شود و این عامل باعث می‌شود تا فرایند یادگیری ماشین به‌روزتر شود و دقت آن افزایش پیدا کند. (بورکوف، ۲۰۱۹)

یادگیری ماشین کاربردهای گوناگونی در حوزه‌های مختلف دارد، کاربردهایی مثل تشخیص چهره، تشخیص گفتار، سامانه توصیف‌گر و خدمات مالی که باعث افزایش سرعت و دقت در روند کاری می‌شود. شرکت‌های بزرگی مثل نتفیلیکس، ویمو، فیسبوک و گوگل هم از این شاخه محبوب در روند کاری خدماتشان استفاده می‌کنند. (تاولی و لورنز، ۲۰۱۹)

شبکه عصبی – Neural Networks

شبکه عصبی یکی از درونی‌ترین لایه های هوش مصنوعی است. با استفاده از الگوریتم های شبکه های عصبی میتوان مدل‌های پیچیده و مختلف را طراحی و شناسایی کرد. یکی از مثال‌هایی که میتوان در مورد شبکه عصبی زد این است که به یک کودک یاد بدهیم که چگونه رنگ‌ها را از یکدیگر تشخیص دهد و این مورد باعث می‌شود تا کودک بعد از مدتی توانایی تشخیص رنگ‌ها را بدست آورد و حتی طیف‌های رنگی را از هم بشناسد، این مثال دقیقا همان کاربرد شبکه عصبی در یاد دادن مطالب به ماشین و سیستم است. شبکه عصبی قابلیت طبقه بندی کردن بصورت دقیق را دارد بطوری که ورودی‌ها را به یک یا چندین خروجی تبدیل کرده و گستره و دامنه خروجی‌ها را به کلاس‌های متفاوت جداسازی می‌کند. (روتمن، ۲۰۲)

شبکه عصبی از بافت‌هایی به نام نورون تشکیل شدند که با بکارگیری نیروی الکترومغناطیسی در راستای حل یک مسئله یا مشکل، با یکدیگر هماهنگ عمل می‌کنند و در نتیجه اطلاعات را انتقال می‌دهند. از اهداف مهم و کاربردهای جالب ایجاد یک شبکه

[۱] Reinforcement Learning

عصبی، پیش بینی کردن است به نوعی که با شبیه‌سازی و مدل‌سازی ویژگی‌های پردازشی مغز انسان و حیوانات، میتوان الگوهای شناخته نشده را شناسایی و بدست آورد. این قابلیت مدل‌های بسیاری دارد که هدف آن مغز انسان است تا بتواند به قدرت تقلید را برسد. نقش شبکه عصبی در جاهایی که نمیدانیم در حال جستجوی چه چیزی هستیم بسیار کمک‌کننده است مثل تطابق چهره، تشخیص دستخط، راندن خودکار اتومبیل و غیره. (تاولی و لورنز، ۲۰۱۹)

بینایی ماشین – Machine Vision

از گسترده‌ترین حوزه های هوش مصنوعی، بینایی ماشین است. اگر بخواهیم این شاخه از هوش مصنوعی را به زبان ساده تعریف کنیم یعنی از طریق بینایی ماشین با استفاده از پردازش دو بعدی می‌تواند یک دنیای سه بعدی را ایجاد و بازسازی کند، مفهوم آن به این معناست که سیستم‌های رایانه‌ای به کمک دوربین ببینند و درک کنند. در بینایی ماشین به گسترش مفاهیمی از سیستم‌های هوشمند اشاره می‌کند که با استفاده از عکس‌ها، اطلاعات دقیق را استخراج می‌کند. از بینایی ماشین در صنایعی که بصورت شبانه‌روزی نیاز به بررسی دارد که سرعت پردازش به شدت بالایی داشته باشد، استفاده می‌شود. (بورکوف، ۲۰۱۹)

طی سال‌های اخیر از هوشمندی بینایی ماشین در صنایع پیشرفته‌ای همچون خطوط تولید کارخانه‌ها جهت کنترل کیفی محصولات استفاده می‌شود. دلایلی که باعث می‌شود تا از تکنولوژی بینایی ماشین استفاده کرد، مواردی همچون سرعت فوق‌العاده بالا، هزینه نگهداری خیلی کم، خطای به شدت پایین، عدم نیاز به حضور اپراتور بصورت شبانه‌روزی و بسیاری از موارد دیگر که باعث شده است تا صنعت‌های مختلف و کارخانه‌های هوشمند به این فناوری جدید و قدرتمند روی بیاورند. یکی از مثال‌هایی که میتوان از تکنولوژی بینایی ماشین زد این است که دستگاهی طراحی و اختراع شده است که با استفاده از پردازش تصویر موجود در بینایی ماشین، توانایی تشخیص نان‌های پخته شده را از پخته نشده دارد و آن‌ها را از یکدیگر جداسازی می‌کند. (روتمن، ۲۰۲)

سامانه های خبره – Expert System

تا به اینجا تمامی شاخه‌های هوش مصنوعی که مورد بررسی قرار دادیم، بر روی اطلاعات و داده‌ها کار می‌کردند اما سامانه های خبره، نرم‌افزارهایی هستند که آگاهی، فهم و دانش

انسانی را در پایگاه داده‌های خود نگهداری و ذخیره می‌کنند. در واقع سامانه های خبره از سیستم‌های کامپیوتری مبتنی بر هوش مصنوعی تشکیل شدند که قابلیت توانایی یادگیری و تصمیم‌گیری دارند و همین امر باعث شده است تا سامانه های خبره بصورت یک دستیار به کاربران توصیه‌های کارشناسانه کند. (بورکوف، ۲۰۱۹)

سامانه های خبره جهت تصمیم‌گیری می‌بایست آگاهی و دانش بدست آورده را در یک قالب مرتبط و مناسب به نمایش دربیاورد و مدیریت کند چون این اطلاعات باید از لحاظ اصالت، اعتبارسنجی بشوند تا داده‌های غلط به سیستم وارد نشود و از نتایج اشتباه جلوگیری شود. یکی از ویژگی‌های منحصر به فرد سامانه های خبره این است که می‌توانند دلایلی که منجر به نتیجه می‌شود را شرح بدهند چون از شیوه‌های ابتکاری به جای روش‌های الگوریتمی استفاده می‌کند. (بورکوف، ۲۰۱۹)

سامانه های خبره از منطق if-then برای حل مسائل و مشکلات پیچیده پیروی می‌کنند و همین موضوع باعث شده است تا از شیوه‌های رایج و مطرح برنامه نویسی استفاده نکنند. تکنولوژی سامانه های خبره در کارهایی همچون بررسی وام‌های بانکی، پردازش سیستم‌های پزشکی، مدیریت و کنترل اطلاعات، کشف و شناسایی ویروس‌ها و غیره کاربرد دارند. (روتمن، ۲۰۲)

پردازش زبان طبیعی – Natural Language Processing

پردازش زبان طبیعی به توانایی درک گفتار انسان می‌پردازد. از کلیدی‌ترین کاربردهای هوش مصنوعی، پردازش زبان طبیعی است که بر پایه یادگیری ماشین می‌باشد. این تکنولوژی به کسب‌وکارهایی کمک می‌کند که بصورت مداوم با انبوهی از متن‌های بدون ساختار همچون پیام‌ها، ایمیل‌ها، رزومه‌ها و غیره سروکار دارند و باعث می‌شود تا این فرایندها سریع‌تر و دقیق‌تر انجام شوند. (تاولی و لورنز، ۲۰۱۹)

پردازش زبان طبیعی به برقراری ارتباط زبان انسانی با کامپیوترها اشاره دارد که به توانایی درک زبان انسان توسط کامپیوتر می‌پردازد. از اهداف مهم پژوهشگران و متخصصان حوزه هوش مصنوعی این است که با استفاده از قابلیت پردازش زبان طبیعی، نرم‌افزارهایی را طراحی کنند که قدرت درک و فهمیدن زبان انسانی را در موضوعات گوناگون داشته باشد. در این بین باید به این نکته اشاره کرد که هدف نهایی هوش بشری برای استفاده

از توانایی پردازش زبان طبیعی، فقط درک زبان طبیعی نیست اما عدم درک آن برای سیستم‌های رایانه‌ای، از ویژگی‌ها و قابلیت‌های کامپیوترها می‌کاهد. (بورکوف، ۲۰۱۹)
در همین راستا، متخصصین این حوزه با تلاش‌های بسیار، توانستند سیستم‌هایی را طراحی کنند که زبان طبیعی انسان را درک کند اما این سیستم‌ها هنوز به سطحی نرسیدند که قدرت و توانایی درک به شدت بالایی از زبان طبیعی انسان‌ها داشته باشند و بتوانند با بشر به راحتی صحبت و گفتگو کنند. در پردازش زبان طبیعی فقط تجزیه و تحلیل واژه‌ها و جملات کافی نیست بلکه سیستم‌های رایانه‌ای باید متوجه نوع موضوع و محتوایی که به آن داده می‌شود بشوند که این قابلیت در مواردی محدود امکان اجرایی شدن دارد. (تاولی و لورنز، ۲۰۱۹)
از مثال‌هایی که میتوان در مورد کاربرد و نقش پردازش زبان طبیعی زد، این است که کامنت‌های یک فیلم را بررسی کند و بر اساس تجزیه و تحلیلی که از متن کامنت بدست می‌آورد، تشخیص بدهد که مثبت یا منفی بوده است. مثال دیگر از این تکنولوژی بررسی محتوای مطالب کاربران در فضای مجازی است که بتواند بر اساس قوانین آن شبکه اجتماعی، محتواهای منتشر شده را از یکدیگر شناسایی کند. (روتمن، ۲۰۲)

الگوریتم ژنتیک – Genetic Algorithm

الگوریتم ژنتیک از شاخه های هوش مصنوعی است که به کمک آن میتوان برنامه‌های کامپیوتری که با موضوعاتی زیستی ارتباط دارند، طراحی کرد. برنامه نویسی الگوریتم ژنتیک توسط گروه جان کوزا (John Koza) توسعه داده شده است، از برنامه نویسی الگوریتم ژنتیک برای طراحی و حل مسئله برنامه‌های جمعیتی، الگوشناسی، روباتیک، کنترل جمعیت، بهینه‌سازی، تئوری بازی‌ها و غیره میتوان استفاده کرد. (بورکوف، ۲۰۱۹)
از اهداف الگوریتم ژنتیک، حل راحت و آسان مسائل مربوطه است که با استفاده از الگوریتم های ژنتیک در راستای فرایند تکامل طبیعی موجودات زنده به کار گرفته می‌شود.
در حقیقت سیستم‌هایی که از الگوریتم های ژنتیک پیروی می‌کنند با استفاده از اصل انتخاب طبیعی داروین برای پیدا کردن فرمول بهینه جهت پیش‌بینی یا تطبیق دادن الگوهای موجود استفاده می‌کنند و به مرور زمان به تکامل می‌رسند. (تاولی و لورنز، ۲۰۱۹)

رشته هوش مصنوعی در مقطع کارشناسی ارشد

رشته هوش مصنوعی در بسیاری از دانشگاه‌های کشورهای دنیا در مقطع کارشناسی ارشد و دکترا ارائه می‌شود که علاقه‌مندان به این رشته می‌توانند در مقطع تحصیلات تکمیلی با رشته هوش مصنوعی آشنا شوند. افرادی که علاقه دارند تا در رشته هوش مصنوعی تحصیل کنند باید از طریق کنکور کارشناسی ارشد وارد رشته هوش مصنوعی شوند. در سال‌های اخیر با توجه به فراگیری علم هوش مصنوعی، بسیاری از افراد به اهمیت و ارزش رشته هوش مصنوعی پی بردند و در نتیجه استقبال بسیاری از دانشجویان و فارغ‌التحصیلان از ادامه تحصیل در رشته هوش مصنوعی شکل گرفت. (بورکوف، ۲۰۱۹) در سال‌های اخیر شاهد افزایش شرکت‌کنندگان در کنکور کارشناسی ارشد برای ادامه تحصیل در رشته هوش مصنوعی هستیم که همین علت باعث شده است تا قبولی در رشته کارشناسی ارشد هوش مصنوعی نسب به سایر گرایش‌ها به شدت سخت‌تر شود و فضای رقابتی در رشته هوش مصنوعی شکل بگیرد. اما با وجود وضعیت سختگیرانه قبولی در رشته هوش مصنوعی، بسیاری این بهانه را می‌آورند که قبولی در رشته هوش مصنوعی سخت و غیرممکن است ولی این دلایل قابل قبول و پذیرفته نیست، زیرا بسیاری از علاقه‌مندان ورود به این رشته با توجه به اینکه رشته‌شان در مقطع کارشناسی با علوم و مهندسی کامپیوتر ارتباطی ندارد و در دانشگاه‌های آزاد، پیام نور و غیرانتفاعی تحصیل کردند با یک برنامه‌ریزی دقیق و درست همراه با پشتکار و استمرار توانستند در یکی از بهترین دانشگاه‌های ایران، مشغول به ادامه تحصیل در رشته هوش مصنوعی شوند. (تاولی و لورنز، ۲۰۱۹)

رشته هوش مصنوعی در مقطع کارشناسی ارشد دارای دروسی همچون نظری، عملی، پژوهشی و تحقیقاتی است که همگی مرتبط با دنیای کامپیوتر و سیستم‌های مرتبط با کامپیوتر هستند. دانشجویان رشته هوش مصنوعی در طی ادامه تحصیلاتشان با درس‌هایی مثل هوش مصنوعی پیشرفته، تئوری و منطق فازی، شبکه های عصبی، پردازش زبان انسان و ... آشنا می‌شوند. از اهداف و قابلیت‌های رشته هوش مصنوعی میتوان به تحلیل اطلاعات، استدلال، یادگیری ماشین، بینایی ماشین، درک گفتار زبان کامپیوتر اشاره کرد. (بورکوف، ۲۰۱۹)

دانشجویانی که قصد دارند در رشته هوش مصنوعی در مقطع کارشناسی ارشد مشغول به تحصیل شوند، باید از مباحث پیش زمینه‌ای در رشته کامپیوتر برخوردار باشند که این مباحث در دروسی همچون مهندسی نرم‌افزار ۱ و ۲، سیستم‌های عامل، نظریه زبان‌ها و ماشین‌ها، طراحی الگوریتم، معماری کامپیوتر، طراحی کامپایلر، ساختمان داده‌ها، منطق و نظریه مجموعه‌ها، پایگاه داده‌ها، ریاضیات گسسته، ساختمان گسسته، زبان‌های برنامه سازی، هوش مصنوعی، مدار منطقی، نظریه گراف، ذخیره و بازیابی دیتا، زبان تخصصی مهندسی کامپیوتر و برخی دروس که بصورت اختیاری ارائه می‌شوند، می‌باشد. (روتمن، ۲۰۲)

کاربرد هوش مصنوعی در امنیت، تهدید یا فرصت؟

کاربرد هوش مصنوعی در امنیت، تهدید یا فرصت؟ پاسخ این سوال، به یک مساله مهم در جامعه امروزی تبدیل شده، چراکه تکنولوژی اطلاعات و ارتباطات به سرعت در حال پیشرفت است. این پیشرفت با خودش چالش‌ها و تهدیداتی برای امنیت سایبری به وجود آورده است. هکرها و مهاجمان با استفاده از روش‌های هوشمندانه و پیچیده، به سیستم‌ها و داده‌های حساس نفوذ می‌کنند که در این میان، هوش مصنوعی به عنوان یک ابزار قدرتمند در پاسخ، پیشگیری و تقویت امنیت سایبری می‌تواند نقش بسیار مهمی را ایفا کند. (بورکوف، ۲۰۱۹)

به راستی هوش مصنوعی چگونه به ما کمک می‌کند تا در دنیای دیجیتال امنیت خود را تضمین کنیم؟ چگونه الگوریتم‌ها و مدل‌های هوش مصنوعی می‌توانند به تشخیص و پیشگیری از تهدیدهای سایبری کمک کنند؟ چگونه هوش مصنوعی به بهبود حفاظت از حریم شخصی و اطلاعات ما در دنیای دیجیتال کمک می‌کند؟ چالش‌ها و فرصت‌های پیش روی ما چیست و هوش مصنوعی چگونه می‌تواند راهنمای ما در حل این چالش‌ها باشد؟

امنیت سایبری چیست؟

بهتر است قبل از صحبت درباره سوال "کاربرد هوش مصنوعی در امنیت سایبری، تهدید یا فرصت؟" کمی راجع‌به خود امنیت سایبری صحبت کنیم و بدانیم که معنی درست این واژه چیست و از چه اجزایی تشکیل شده است. (روتمن، ۲۰۲)

به طورکلی وقتی از دستگاه‌های متصل به اینترنت محافظت می‌کنیم، به آن امنیت سایبری گفته می‌شود که این محافظت شامل سخت‌افزار، نرم‌افزار و داده‌ها در برابر تهدیدات مجرمان سایبری است. در حقیقت افراد و سازمان‌ها، از این روش برای محافظت در برابر دسترسی غیرمجاز به مراکز داده و سایر سیستم‌های رایانه‌ای استفاده می کنند. این هم بدانید که افراد فعال در بخش امنیت سایبری، بهترین آموزش‌ها برای شناسایی و جلوگیری از هرگونه حمله به سیستم را نیاز دارند. در واقع داشتن یک استراتژی در امنیت سایبری برای عملکرد خوب در برابر حملات مخربی که به منظور دسترسی، دستکاری، حذف، اخاذی یا تخریب داده‌های یک سازمان یا سیستم‌های فردی و سرقت داده‌های حساس ایجاد می‌شوند، مهم‌ترین عامل در بخش امنیت سایبری است که باید به اندازه کافی قدرتمند باشد. (بورکوف، ۲۰۱۹)

اهمیت امنیت سایبری چیست؟

باتوجه به تعریف این واژه باید گفت که امروزه، تعداد کاربرانی که از دستگاه‌ها و برنامه‌ها استفاده می‌کنند یا شرکت‌های مدرنی که حجم زیادی از داده‌ها را تولید می‌کنند، دارای داده‌های بسیار حساس یا محرمانه‌ای هستند که میزان آن به طور قابل توجهی افزایش یافته است. بنابراین در اینجا اهمیت امنیت سایبری مطرح می‌گردد، چراکه سرقت داده‌ها در سیستم‌ها همچنان در حال رشد است. (تاولی و لورنز، ۲۰۱۹)

در حقیقت افزایش حجم و پیچیدگی بیشتر در روش‌هایی که توسط مهاجمان سایبری از طریق تکنیک‌های حمله استفاده می‌شود، مشکلات بسیاری را به وجود آورده که جلوگیری از این موضوع، جز با تکنیک امنیت سایبری امکان‌پذیر نیست. (روتمن، ۲۰۲)

اجزای امنیت سایبری

در خصوص این مساله، حوزه امنیت سایبری را می‌توان بر اساس نوع امنیتی که روی دستگاه‌ها ایجاد می‌کنند، به اجزای مختلفی تقسیم کرد که ادغام همه آن‌ها در یک شرکت برای رسیدن به موفقیت برنامه امنیت سایبری، بسیار مهم است. پس اجزای امنیت سایبری به شرح زیر است: (بورکوف، ۲۰۱۹)

- امنیت برنامه
- امنیت اطلاعات یا داده ها
- امنیت شبکه

- بازیابی بلایا و برنامه‌ریزی تداوم کسب و کار
- امنیت عملیاتی
- امنیت ابری
- امنیت زیرساخت های حیاتی
- امنیت فیزیکی
- آموزش کاربر نهایی
- کار در زمینه امنیت سایبری
- مزایای امنیت سایبری

می توان گفت امنیت سایبری بخاطر دلایلی که در ادامه نام می‌بریم، مزایای بسیاری دارد که البته این موارد شامل گزینه‌های زیر هستند: (روتمن، ۲۰۲)

- از کسب و کارها در برابر حملات سایبری و نقض داده‌ها محافظت می‌شود. علاوه‌برآن از داده‌ها و شبکه‌ها نیز محافظت می‌گردد.
- از دسترسی غیرمجاز کاربر جلوگیری می‌شود.
- از افراد برای در استفاده از دستگاه‌ها و کاربران نهایی محافظت می‌گردد.
- دارای انطباق با مقررات است.
- تداوم تجارت را تضمین می‌کند.
- اعتماد به شهرت یک سازمان را بهبود می‌بخشد.
- چالش‌های برتر امنیت سایبری

جالب است بدانید که امنیت سایبری به طور مداوم توسط هکرهایی که مسئول از دست دادن داده‌ها هستند به چالش کشیده می شود. علاوه‌براین، حریم خصوصی، مدیریت ریسک و تغییر استراتژی‌های امنیت سایبری نیز یک تهدید هستند و انتظار نمی‌رود که تعداد حملات سایبری، در آینده کاهش یابد زیرا افراد بیشتری به اینترنت دسترسی پیدا می‌کنند. همچنین ورود تکنولوژی اینترنت اشیا (IoT) نیز نقاط ورودی برای حملات ایمن‌سازی شبکه‌ها و دستگاه‌ها را افزایش می دهد. (بورکوف، ۲۰۱۹)

در واقع تحولات خطرات امنیتی، یکی از مشکل‌سازترین عناصر امنیت سایبری است که با ظهور فن‌آوری‌های جدید، از آن به روش‌های متفاوتی استفاده می‌شود و راه‌های حمله

جدید را توسعه می‌یابد. پس سوال این است که چگونه می‌توان از خطرات و چالش‌های امنیت سایبری جلوگیری کرد؟ (تاولی و لورنز، ۲۰۱۹)

نقش هوش مصنوعی و ورود آن در امنیت سایبری

اکنون نوبت به پاسخ سوال " کاربرد هوش مصنوعی در امنیت، تهدید یا فرصت؟ " است. همانطور که گفتیم حفظ امنیت سایبری به یک چالش برای همه سازمان‌ها تبدیل شده است، چراکه رویکردهای سنتی دیگر یک تاکتیک کافی برای محافظت از سیستم‌ها در برابر بزرگترین تهدیدات شناخته شده امروزی نیست. همچنین برای همگام شدن با خطرات امنیتی در حال تغییر، یک رویکرد فعال‌تر و سازگارتر، ضروری است که در اینجا بحث استفاده از هوش مصنوعی در امنیت سایبری به میان آمده و از آن به عنوان یک راه سودمند استفاده می‌شود. (تاولی و لورنز، ۲۰۱۹)

در واقع هوش مصنوعی می‌تواند به کارشناسان امنیتی برای تجزیه، تحلیل، مطالعه و درک جرایم سایبری، کمک کند. همچنین فناوری‌هایی که شرکت‌ها برای مبارزه با مجرمان سایبری استفاده می‌کنند را بهبود می‌بخشد و به آن‌ها کمک می‌کند تا اطلاعات مشتریان را ایمن نگه دارند. (روتمن، ۲۰۲)

البته ناگفته نماند که هوش مصنوعی می‌تواند به عنوان یک منبع بسیار جامع در امنیت سایبری محسوب شود و عملا در هر برنامه کاربردی، قابل استفاده نباشد و مهم‌تر از همه اینکه، می‌تواند به عنوان یک سلاح جدید و در عین حال خطرناک برای تقویت مجرمان سایبری در تکنیک‌های خود و بهبود حملات سایبری باشد. پس در ادامه همراه درسمن باشید تا بیشتر درخصوص کاربردها، تهدیدات و چالش‌های هوش مصنوعی در حوزه امنیت سایبری صحبت کنیم. (بورکوف، ۲۰۱۹)

کاربرد هوش مصنوعی در امنیت سایبری

پس در همان ابتدا یک توضیح جامع از سوال " کاربرد هوش مصنوعی در امنیت، تهدید یا فرصت؟ " را دریافتیم و متوجه شدیم که استفاده از هوش مصنوعی در امنیت سایبری هم می‌تواند کاربردی باشد و هم تهدیدآمیز؛ پس بیایید در ابتدا به کاربردهای مهم و جذاب این علم پرداخته و بعد درخصوص چالش‌ها و تهدیدات هوش مصنوعی در امنیت سایبری صحبت کنیم. از کاربردهای این علم و تکنولوژی‌های هوشمند آن می‌توان به موارد زیر اشاره کرد: (تاولی و لورنز، ۲۰۱۹)

تشخیص تهدیدات با استفاده از هوش مصنوعی

یکی از کاربردهای اصلی هوش مصنوعی در امنیت سایبری، تشخیص تهدیدات است. سیستم‌های هوش مصنوعی با تحلیل الگوهای عملکردی ناشناخته و شناسایی رفتارهای غیرمعمول، قادر هستند به طور خودکار تهدیدات را شناسایی و اعلام کنند. این ویژگی به ارتقا سرعت و دقت در تشخیص حملات کمک می‌کند. (بورکوف، ۲۰۱۹)

پیش‌بینی حملات و تشویق به پژوهش

هوش مصنوعی می‌تواند با تجزیه و تحلیل داده‌های حجیم و پیچیده، الگوهای آتی حملات را پیش‌بینی کند. در واقع هوش مصنوعی به اپراتورهای امنیتی این اطمینان را می‌دهد که با استفاده از اطلاعات پیشین و شناخت الگوهای حملات، می‌توانند برنامه‌های پیشگیری موثرتری را پیاده‌سازی کنند. (روتمن، ۲۰۲)

اتوماسیون در پاسخ به حملات

هوش مصنوعی به سیستم‌ها این امکان را می‌دهد تا به صورت اتوماتیک به حملات پاسخ دهند. از جمله مزایای این رویکرد، افزایش سرعت در واکنش به حملات و کاهش وابستگی به نیروی انسانی در مواجهه با حملات سایبری است. (تاولی و لورنز، ۲۰۱۹)

افزایش دقت در تصمیم‌گیری‌های امنیتی

هوش مصنوعی با استفاده از الگوریتم‌ها و مدل‌های یادگیری عمیق، قادر به ارائه تصمیم‌گیری‌های دقیق‌تر و هوشمندانه‌تر در زمینه امنیت سایبری است که این قابلیت به مدیران امنیتی کمک می‌کند تا با اطمینان بیشتر، تصمیماتی اثربخش در مواجهه با تهدیدات امنیتی بگیرند. (بورکوف، ۲۰۱۹)

تطبیق پویا با تهدیدات

یکی از نکات مهم برای کاربرد هوش مصنوعی در امنیت سایبری آینده، توانایی سیستم‌ها در تطبیق پویا با تهدیدات جدید است. تهدیدات سایبری به سرعت تغییر می‌کنند و نیاز به یک سیستم هوش مصنوعی دینامیک و قابل تطبیق داریم که بتواند به سرعت واکنش نشان دهد.

الگوریتم‌ها و مدل‌های یادگیری ماشینی با توانایی تطبیق بهبود یافته و آموزش داده‌های جدید ، این تطبیق پویا را تسهیل می‌کنند. (روتمن، ۲۰۲)

مدیریت ریسک مبتنی بر داده

اطلاعات زیادی که توسط سیستم‌های هوش مصنوعی جمع‌آوری می‌شوند، به عنوان یک منبع قوی برای مدیریت ریسک سایبری مورد استفاده قرار می‌گیرد. تحلیل داده‌های ساختاری و غیرساختاری، تشخیص الگوهای عجیب و تشکیل پایگاه داده قدرتمند، به سازمان‌ها این امکان را می‌دهد تا با بروز تهدیدات، سریع مقابله کنند. استفاده از داده به عنوان یک ابزار اساسی در فرایند تصمیم‌گیری به سازمان‌ها کمک می‌کند تا ریسک‌ها را به بهترین شکل مدیریت کنند. (تاولی و لورنز، ۲۰۱۹)

آگاهی از امنیت در طی چرخه زندگی نرم‌افزارها

در آینده، امنیت نباید به مرحله آخر توسعه نرم‌افزار محدود شود. بلکه، باید از ابتدا تا انتها در تمام چرخه زندگی نرم‌افزارها مدیریت شود. این موضوع شامل توسعه امنیتی نرم‌افزار، تست‌های امنیتی مداوم، به‌روزرسانی‌های امنیتی و مانیتورینگ مداوم برای تشخیص سریع تردد‌های ناخواسته است. بنابراین، هوش مصنوعی می‌تواند در این فرآیندها بهبودهای مهمی از جمله شناسایی خودکار آسیب‌پذیری‌ها و اجرای تست‌های امنیتی، ایجاد کند. (تاولی و لورنز، ۲۰۱۹)

توسعه همکاری‌های صنعتی و بین‌المللی

توسعه همکاری‌های صنعتی و بین‌المللی در زمینه امنیت سایبری یکی از چالش‌های مهم آینده است، چراکه تهدیدات سایبری بی‌مرز هستند و همکاری بین سازمان‌ها، شرکت‌ها، دولت‌ها، و حتی تحقیقات دانشگاهی در سطح جهانی، ضروری است. به همین خاطر یکی دیگر از کاربردهای هوش مصنوعی در امنیت سایبری که می‌تواند نقش بسیار مهمی در تبادل اطلاعات امنیتی، تشخیص الگوهای حملات و ایجاد راهکارهای جمعی، داشته باشد. (روتمن، ۲۰۲)

حفاظت از حریم خصوصی و اخلاق در هوش مصنوعی

همانطور که از هوش مصنوعی برای امنیت سایبری استفاده می‌شود، حفاظت از حریم خصوصی و رعایت اصول اخلاقی نیز بسیار حائز اهمیت است. تضمین کنترل بر داده‌ها و اطمینان از اینکه هوش مصنوعی به نحو مناسب و مسئولانه از اطلاعات حساس استفاده می‌کند، امری اساسی است. بنابراین، تحقیقات و توسعه در زمینه سیاست‌های حفاظت

از حریم خصوصی و ایجاد الگوریتم‌ها و مدل‌هایی که از نظر اخلاقی مطمئن و شفاف باشند، یکی دیگر از کاربردهایی است که همگام با تکنولوژی، ادامه یابد. (بورکوف، ۲۰۱۹)

توسعه راهکارهای پیشگیری از حملات سایبری

راهکارهای پیشگیری از حملات سایبری بسیار اهمیت دارند که در آینده، توسعه رویکردهای هوشمندانه‌تر در این زمینه پیش‌بینی می‌شود. هوش مصنوعی می‌تواند به عنوان یک ابزار قوی در تشخیص آسیب‌پذیری‌ها، مسدودسازی حملات و بهبود امنیت سیستم‌ها و شبکه‌ها مورد استفاده قرار گیرد. توانایی پیشگیری از حملات به صورت هوشمند با استفاده از هوش مصنوعی، به سازمان‌ها این امکان را می‌دهد که بازدهی بیشتری در مقابل تهدیدات سایبری داشته باشند. (روتمن، ۲۰۲)

حفاظت از اینترنت اشیا (IoT)

با افزایش استفاده از اینترنت اشیا، حفاظت از این دستگاه‌های متصل به شبکه اینترنت به یک چالش بزرگ تبدیل شده است که هوش مصنوعی در امنیت سایبری این دستگاه‌ها، می‌تواند نقش مهمی در تشخیص حملات به دستگاه‌های IoT داشته باشد و از آسیب‌پذیری آن‌ها پیشگیری کند. این ابزارها می‌توانند الگوهای ناشناخته رفتارها را شناسایی کرده و حملات را متوقف سازند. همچنین می‌توانند مدیریت امنیت دستگاه‌های متصل به اینترنت را بهبود بخشند. (تاولی و لورنز، ۲۰۱۹)

امنیت در زنجیره تامین

امنیت در زنجیره تامین نیز یک جنبه مهم در امنیت سایبری است که نیاز به توجه خاص دارد. هوش مصنوعی می‌تواند در تشخیص تهدیدات زنجیره تامین، مانیتور کردن ارتباطات و حفاظت از اطلاعات حساس در طول این زنجیره، ایفا نقش کند. در واقع هوش مصنوعی می‌تواند به بهبود و افزایش امنیت در تمام مراحل تولید و توزیع تا مصرف و مدیریت محصولات زنجیره تامین، کمک کند. (بورکوف، ۲۰۱۹)

توسعه تکنولوژی‌های تشخیص تهدیدات در زمینه هوش مصنوعی

یکی دیگر از راهکارهای تامین امنیت با هوش مصنوعی، توسعه تکنولوژی‌های تشخیص تهدیدات است. از الگوریتم‌های یادگیری ژرف گرفته تا سیستم‌های تشخیص ناشناخته، قادر به شناسایی الگوهای حملات جدید و پیچیده خواهند بود. همچنین، ترکیب هوش

مصنوعی با تحلیل داده‌های ریز و بزرگ (Big Data)، می‌تواند به بهبود تشخیص تهدیدات و ارائه پاسخ‌های سریعتر و موثرتر کمک کند. (بورکوف، ۲۰۱۹)

هوش مصنوعی و امنیت سایبری برای سیستم‌های تشخیص تهدیدات مبتنی بر رفتار سیستم‌های تشخیص تهدیدات مبتنی بر رفتار با تحلیل الگوهای عادی رفتاری سیستم‌ها و کاربران، تغییرات مشکوک را شناسایی و در توسعه و بهبود این سیستم‌ها، نقش اساسی ایفا کند. در حقیقت هوش مصنوعی در امنیت سایبری این موضوع، با استفاده از الگوریتم‌های یادگیری ماشینی تا سیستم‌های تصمیم‌گیری هوشمند می‌تواند به صورت پویا با تغییرات الگوهای رفتاری و تهدیدات سازمان‌ها، هماهنگ شود. (روتمن، ۲۰۲)

حل مسائل تراز اولیه

هوش مصنوعی می‌تواند در حل مسائل تراز اولیه (First Level Analysis) نقش مهمی ایفا کند. هوش مصنوعی می‌تواند به تحلیل اولیه و سریع داده‌ها برای تشخیص حملات ساده تا شناسایی الگوهای مشکوک در داده‌های ورودی، کمک کند. این قابلیت می‌تواند زمان پاسخ به حملات را بهبود بخشیده و امکان پیشگیری از گسترش حملات را فراهم کند. (بورکوف، ۲۰۱۹)

ارتقا تکنولوژی‌های گزارشگیری و تحلیل رویدادها

یکی دیگر از کاربردهای هوش هوش مصنوعی در امنیت سایبری، ارتقا تکنولوژی‌های گزارشگیری و تحلیل رویدادها است. این تکنولوژی می‌تواند یک ابزار قوی برای تحلیل داده‌های زمان‌واقعی و افزایش دقت در تشخیص رویدادهای مشکوک داشته باشد و مدیریت واکنش به حوادث و حملات سایبری را بهبود بخشد تا اطلاعات دقیق‌تری در مورد امنیت سیستم‌ها گزارش شود. (تاولی و لورنز، ۲۰۱۹)

مزایای هوش مصنوعی در امنیت سایبری

گرچه کاربردهای هوش مصنوعی در امنیت سایبری بسیار گسترده است اما دیگر می‌خواهیم از مزایای تامین امنیت با هوش مصنوعی صحبت کنیم که به شرح زیر است:

- هوش مصنوعی با گذشت زمان هوشمندتر می شود:

فناوری هوش مصنوعی همانطور که از نامش پیداست به دلیل توانایی آن در بهبود امنیت شبکه، کارآمد و هوشمند است. در واقع هوش مصنوعی با به کارگیری از یادگیری ماشین

و یادگیری عمیق خود، الگوهای موجود در شبکه را شناسایی می شود و سپس آنها را در کنار هم قرار می دهد تا متوجه شود که آیا انحرافاتی وجود دارد یا حادثه امنیتی در ترافیک عادی رخ داده است؟ در نهایت، پس از تجزیه و تحلیل ترافیک، به آنها پاسخ می دهد، به همین دلیل است که می‌گوییم هوش مصنوعی با گذر زمان و ارتقا الگوریتم‌های خود، هوشمند می‌شود. (روتمن، ۲۰۲)

- هوش مصنوعی در امنیت سایبری به شناسایی تهدیدات ناشناخته کمک می‌کند:

به دلیل افزایش حملات بدافزار در مهندسی‌های پیچیده، برای جلوگیری از آسیب رساندن حملات جدید به سیستم‌ها نیاز به استفاده از راه حل‌های مدرن است، چراکه مهاجمان روش‌های جدیدی را برای آسیب رساندن به سیستم‌ها امتحان می‌کنند. (روتمن، ۲۰۲)

در نتیجه به منظور شناسایی و جلوگیری از تهدیدات ناشناخته از تخریب زیرساخت شبکه یک سازمان، هوش مصنوعی در امنیت سایبری یکی از بهترین ترکیب‌ها برای فناوری‌های امنیتی است. (بورکوف، ۲۰۱۹)

- هوش مصنوعی در امنیت سایبری، می‌تواند داده‌های زیادی را مدیریت کند:

شناسایی هر گونه تهدید احتمالی که به عنوان یک فعالیت عادی، ثابت می کند که تامین امنیت با هوش مصنوعی، بهترین راه حل است زیرا این تکنولوژی می‌تواند حجم زیادی از داده‌ها را خوانده و آن‌ها را تجزیه و تحلیل می کند تا هرگونه تهدید احتمالی به صورت خودکار شناسایی کند. علاوه‌براین هر تهدیدی که ممکن است در ترافیک وجود داشته باشد را شناسایی می‌کند. (تاولی و لورنز، ۲۰۱۹)

- هوش مصنوعی می تواند آسیب پذیری در امنیت سایبری را بهتر مدیریت کند:

هوش مصنوعی سریع است و می‌تواند به ما کمک کند تا سیستم‌ها را سریع‌تر از پرسنل امنیت سایبری ارزیابی و در نتیجه بار کاری را کاهش داد. همچنین توانایی حل مشکلات، چندین برابر افزایش می‌دهد، چراکه این تکنولوژِ قادر است نقاط ضعف سیستم‌های کامپیوتری و شبکه‌های تجاری را شناسایی کرده و به کسب‌وکارها کمک کند تا بر روی آن تمرکز کنند. پس هوش مصنوعی وظایف مرتبط با مدیریت آسیب پذیری و ایمن سازی سیستم های تجاری را در امنیت سایبری به موقع ممکن می‌سازد. (روتمن، ۲۰۲)

شاید این سوال هم در ذهن شما ایجاد شده باشد که هوش مصنوعی با این همه توانایی در بحث امنیت می‌تواند باعث تهدید این مساله شود؟ در حقیقت می‌خواهیم به بخش دوم این سوال یعنی "کاربرد هوش مصنوعی در امنیت سایبری، تهدید یا فرصت؟" بپردازیم که می‌تواند برای شما عزیزان نیز جالب و قابل تامل باشد. (تاولی و لورنز، ۲۰۱۹) در ابتدای پاسخ به این سوال باید بگوییم بله؛ هوش مصنوعی در امنیت سایبری نیز می‌تواند چالش‌هایی را وجود دارد و آن را به یک عامل تهدید کننده تبدیل کند که از مهم‌ترین آن‌ها باید به موارد زیر اشاره کرد: (تاولی و لورنز، ۲۰۱۹)

۱. تطبیق مهاجمان با سیستم‌های هوش مصنوعی و انجام حملات مبتنی بر آن

یکی از اصلی‌ترین چالش‌ها و شکست امنیت با هوش مصنوعی، توانایی مهاجمان در تطبیق با سیستم‌های هوش مصنوعی و انجام حملات مبتنی بر آن است. به علاوه، مسائل حریم خصوصی نیز می‌تواند یک موضوع مهم در استفاده از تکنولوژی‌های هوش مصنوعی برای امنیت سایبری باشد. (روتمن، ۲۰۲)

۲. توازن میان انسان و هوش مصنوعی

یک جنبه دیگر از توسعه هوش مصنوعی در امنیت سایبری، توازن میان نقش انسان و هوش مصنوعی است. استفاده از هوش مصنوعی برای اتوماسیون و اتخاذ تصمیمات اتوماتیک می‌تواند بهبود قابل توجهی در سرعت پاسخگویی به حملات داشته باشد اما در عین حال، حضور انسان در تصمیم‌گیری‌ها و تجزیه و تحلیل موقعیت‌های پیچیده همچنان ضروری است. (بورکوف، ۲۰۱۹)

تعیین توانمندی‌های هرکدام از این دو عامل و تعادل بین آنها، یکی از چالش‌های مهم در طراحی سیستم‌های امنیتی با هوش مصنوعی است. از این‌رو، نیاز به پژوهش و توسعه راهکارهایی که هوش مصنوعی و انسان را به بهترین شکل ممکن در کنار هم قرار دهد به شدت احساس می‌شود. (تاولی و لورنز، ۲۰۱۹)

۳. آموزش و آگاهی عمومی

آموزش و آگاهی عمومی از دیگر جنبه‌های مهم در امنیت سایبری با هوش مصنوعی است که افراد باید اطلاعات لازم در مورد تهدیدات سایبری، روش‌های حفاظت و استفاده امن از تکنولوژی‌های هوش مصنوعی را به دست آورند و یه یک چالش ر استفاده از این تکتولوژی برای بخش امنیت سایبری تبدیل شده است. (تاولی و لورنز، ۲۰۱۹)

در حقیقت این مسئله نیازمند همکاری دولت، صنعت و موسسات آموزشی است تا بتوانند با یکدیگر در جهت افزایش آگاهی عمومی و ایجاد فرهنگ امنیت سایبری همکاری نمایند. تبعیض ناشناخته هوش مصنوعی ممکن است در برخی موارد تهدیداتی که از قبل شناخته نشده‌اند را تشخیص ندهد و این مسئله می‌تواند به عنوان یک چالش در حوزه تشخیص تهدیدات جدید مطرح شود. (روتمن، ۲۰۲)

درک اشتباه

مدل‌های هوش مصنوعی ممکن است درک اشتباهی از ورودی‌ها داشته باشند و نتایج نادرستی ارائه دهند که ای موضوع در مواجهه با حملات ناشناخته یا تغییرات ناگهانی در محیط سایبری به چالش کشیده می‌شود. (بورکوف، ۲۰۱۹)

زمان و هزینه

پیاده‌سازی و مدیریت سیستم‌های هوش مصنوعی ممکن است زمان‌بر و گران باشد. همچنین، نیاز به منابع زیادی برای آموزش مدل‌ها و به‌روزرسانی آن ها مطرح است.

اعتبار پذیری

اعتبار پذیری مدل‌های هوش مصنوعی و قابلیت تضمین صحت نتایج آنها ممکن است چالش‌هایی را در مواجهه با تصمیمات امنیتی حساس، ایجاد کند. (تاولی و لورنز، ۲۰۱۹)

معرفی ابزارها و الگوریتم‌های هوش مصنوعی در امنیت سایبری

هوش مصنوعی برای انجام نقش‌های مختلف در امنیت سایبری از الگوریتم‌ها، مدل‌های یادگیری ماشین و ابزارهای متنوعی استفاده می‌کند.

به همین دلیل ما نیز در درسمن تصمیم گرفتیم که در آخرین بحث از کاربردهای هوش مصنوعی در امنیت سایبری، به معرفی ابزارها و الگوریتم‌های این تکنولوژی بپردازیم که به شرح زیر است: (روتمن، ۲۰۲)

شبکه‌های عصبی

شبکه‌های عصبی عمیق (Deep Neural Networks - DNN) و شبکه‌های عصبی کانولوشنی (Convolutional Neural Networks - CNN) برای تشخیص الگوها و ویژگی‌های خاص در تصاویر و داده‌های ساختار یافته امنیت سایبری مورد استفاده قرار می‌گیرند. (بورکوف، ۲۰۱۹)

الگوریتم‌های یادگیری ماشین

الگوریتم‌های یادگیری ماشین مانند درخت تصمیم (Decision Trees)، ماشین‌های بردار پشتیبان (Support Vector Machines - SVM) و روش‌های یادگیری نظارت شده و نظارت نشده، برای تصمیم‌گیری در مورد داده‌ها و تشخیص الگوهای امنیت سایبری استفاده می‌شوند. (تاولی و لورنز، ۲۰۱۹)

الگوریتم‌های خوشه‌بندی

الگوریتم‌های خوشه‌بندی مانند K-Means و hierarchical clustering برای گروه‌بندی داده‌ها به منظور تشخیص الگوها و تغییرات ناهنجار در امنیت سایبری مورد استفاده قرار می‌گیرد. (روتمن، ۲۰۲)

آمار و احتمالات

روش‌های آماری و احتمالاتی برای تحلیل و پیش‌بینی تغییرات در داده‌ها و احتمال وقوع حوادث ناخواسته استفاده می‌شود. (تاولی و لورنز، ۲۰۱۹)

پردازش زبان طبیعی (NLP)

پردازش زبان طبیعی در زمینه امنیت سایبری برای تحلیل و تفسیر اطلاعات متنی چون تشخیص تهدیدات در متون، تحلیل لاگ‌ها، و تشخیص تلاش‌های مهندسی اجتماعی مورد استفاده قرار می‌گیرد. (بورکوف، ۲۰۱۹)

سیستم‌های تشخیص ناهنجار

سیستم‌های تشخیص ناهنجار با استفاده از مدل‌های آماری و یادگیری ماشین، تغییرات ناهنجار را در سیستم‌ها برای امنیت دستگاه‌ها شناسایی می‌کند. (روتمن، ۲۰۲)

مدیریت هویت و دسترسی

از سیستم‌های مدیریت هویت و دسترسی (IAM) برای شناسایی فعالیت‌های ناعادلانه و دسترسی‌های غیرمجاز استفاده شده که جلوگیری از آنها را مدیریت کنند. (بورکوف، ۲۰۱۹)

در نهایت، تمامی این تکنولوژی‌ها و الگوریتم‌ها به صورت ترکیبی در سیستم‌ها و ابزارهای امنیتی مورد استفاده قرار می‌گیرند تا به صورت جامع و اثربخش در مقابله با تهدیدات سایبری عمل کنند. (تاولی و لورنز، ۲۰۱۹)

پس به طورکلی می‌توان گفت . . .

پس اکنون شما پاسخ "کاربرد هوش مصنوعی در امنیت، تهدید یا فرصت؟" را می‌دانید زیرا که استفاده از هوش مصنوعی در امنیت سایبری به یک فرآیند تحولی در جامعه امروزی تبدیل شده است. به بیان بهتر اینکه، هوش مصنوعی در امنیت سایبری هم می‌تواند به یک فرصت تبدیل شود و هم می‌تواند در کنار کاربردها و اهمیت بالای آن در تامین امنیت، چالش‌هایی را به همراه داشته باشد. (روتمن، ۲۰۲)

در حقیقت هوش مصنوعی در برابر مقابله با تهدیدات پیشرفته گرفته تا تقویت دفاعات سایبری و آموزش ماشینی برای بهبود دقت تشخیص، باعث ارتقا سطح امنیت در مقابل تهدیدات سایبری متنوع و پیچیده شود که البته چالش‌ها و تهدیدات آن نیز، نیاز به توجه دقیق و پایداری از سوی متخصصان امنیت دارد. (بورکوف، ۲۰۱۹)

اگر شما هم می‌خواهیم به عنوان یک متخصص توانمند در هوش مصنوعی فعالیت کنید، می‌توانید از دوره استادی هوش مصنوعی درسمن استفاده کنید. همچنین اگر نیاز به راهنمایی در این زمینه داشتید، حتما با کارشناسان ما در شبکه‌های اجتماعی یا صفحه گفتگو چت آنلاین سایت، ارتباط برقرار کنید. (روتمن، ۲۰۲)

روش تحقیق علمی

روش تحقیق علمی مجموعه‌ای از اصول، مراحل و تکنیک‌های نظام‌مند است که برای جمع‌آوری، تجزیه و تحلیل داده‌ها و رسیدن به نتایج معتبر در یک پژوهش علمی استفاده می‌شود. این روش‌ها برای پاسخ به سوالات پژوهشی و حل مشکلات علمی طراحی شده‌اند و به پژوهشگران کمک می‌کنند تا به طور منطقی و نظام‌مند، فرآیند تحقیقاتی خود را پیش ببرند (بورکوف، ۲۰۱۹)

پیشینه روش تحقیق

پیشینه هوش مصنوعی به کجا بازمی‌گردد؟ هوش مصنوعی ساخت کدام کشور است؟ این‌ها سوالاتی هستند که حداقل یک بار به آن فکر کرده‌ایم. هوش مصنوعی (Artificial Intelligence) یا AI در حال حاضر به یکی از داغ‌ترین موضوعات در حوزه فناوری تبدیل شده است. شاید در ابتدا این‌چنین به نظر برسد که هوش مصنوعی در همین چند سال اخیر پیشرفت کرده و مورد استفاده قرار گرفته است اما در واقع، تاریخچه هوش مصنوعی به اوایل دهه ۱۹۰۰ باز می‌گردد. اگرچه بزرگ‌ترین گام‌ها در دهه ۱۹۵۰ برداشته شد، اما

این کار بدون تلاش متخصصان اولیه در بسیاری از زمینه‌های مختلف امکان‌پذیر نبود. (روتمن، ۲۰۲)

نتیجه گیری

هوش مصنوعی یکی از حوزه‌های پیشرفته و جذاب علوم کامپیوتر است که در دهه‌های اخیر بسیار مورد توجه قرار گرفته است. هوش مصنوعی به ما امکان می‌دهد تا سیستم‌های کامپیوتری را به گونه‌ای طراحی کنیم که بتوانند فعالیت‌های هوشمندانه انجام دهند و وظایفی را انجام دهند که قبلاً نیاز به تفکر و هوش بشری داشته‌اند.

هوش مصنوعی AI یک علم و مهندسی است که علاقه‌مندان زیادی را به تحقیق در این حوزه جلب کرده است. هوش مصنوعی انواع مختلفی از نظر ماهیت و یادگیری شامل Strong AI و Weak AI و Super AI و همچنین انواع دیگری از نظر عملکرد شامل ماشین‌های واکنشی (Reactive Machines)، حافظه محدود (Limited Memory)، نظریه ذهن (Theory of Mind) و خودآگاه (Self-aware) دارد که دستیابی به همه آن‌ها با توجه به فناوری‌های فعلی موجود امکان‌پذیر نیست و هنوز راه طولانی در پیش داریم. (روتمن، ۲۰۲)

به طورکلی می‌توان هوش مصنوعی را روشی برای کارشناسان امنیتی دانست که با کمک آن به تجزیه و تحلیل، مطالعه و درک جرایم سایبری می پردازند. همچنین به بهبود فناوری‌هایی که شرکت‌ها برای مبارزه با مجرمان سایبری استفاده می‌کنند نیز کمک کرده تا داده‌های مشتری را ایمن نگه دارند. هوش مصنوعی آینده امنیت سایبری است زیرا یکفناوری در حال پیشرفت است و حقیقتا انسان‌ها نمی‌توانند مراقب هر حمله‌ای باشند. بنابراین ما در آینده شاهد کاربرد بیشتر هوش مصنوعی در امنیت سایبری خواهیم بود. هوش مصنوعی می‌تواند به کشف و تمرکز خطرات، واکنش مستقیم به حادثه و تشخیص حملات بدافزاری قبل از ورود را کمک کند. همچنین سرعت بهره بردن این تکنولوژی به عنوان یک نوآوری با اولویت بالا، برای بهبود عملکرد گروه‌های امنیتی فناوری اطلاعات در حال ظهور است.

منابع

Rothman, Denis. (2020), Artificial Intelligence By Example: Acquire advanced AI, machine learning, and deep learning design skills, 2nd Edition, Packt Publishing

Taulli, Tom & Lorenz, Julia. (2019) Artificial Intelligence Basics: A Non-Technical Introduction, O'Reilly Media.

Burkov, Andriy. (2019), The Hundred-Page Machine Learning, Amazon. https://www.amazon.com/Hundred-Page-Machine-Learning-Book/dp/199957950X.