مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۹، بهار ۱۴۰۲، ص ۲۲- ۱۴

ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال هشتم)
شماره ۲۹ / بهار ۱۴۰۲ / ص ۲۲- ۱۴

کاربرد هوش مصنوعی و اهمیت آن در امنیت IT

شهرام محمدی
کارشناس ارشد کامپیوتر نرم افزار

نام نویسنده مسئول:
شهرام محمدی

تاریخ دریافت: ۱۴۰۱/۱۲/۲۵
تاریخ پذیرش: ۱۴۰۲/۰۳/۰۳

چکیده

شبکه های عصبی مصنوعی تا حد زیادی ملهم از سیستم های یادگیر طبیعی است که در آنها یک مجموعه پیچیده از نرونهای به هم متصل در کار یادگیری دخیل هستند. انواع مختلفی از مدل‌های محاسباتی تحت عنوان کلی شبکه‌های عصبی مصنوعی معرفی شده اند، که هر یک برای دسته ای از کاربردها قابل استفاده اند و در هر کدام، از وجه مشخصی از قابلیت ها و خواص مغز انسان، الهام گرفته شده است. امروز به قدری استفاده از سیستم های هوشمند، به ویژه شبکه عصبی مصنوعی گسترده شده است، که می توان این ابزارها را، در ردیف عملیات پایه ریاضی و به عنوان ابزارهای عمومی و مشترک طبقه‌بندی کرد. چرا که کمتر رشته دانشگاهی است که نیازی به تحلیل، تصمیم‌گیری، تخمین، پیش بینی، طراحی و ساخت داشته باشد، و در آن از موضوع شبکه های عصبی استفاده نشده باشد. هدف این مقاله بررسی کاربرد هوش مصنوعی و امنیت آن در امنیت IT می‌باشد. این نوع پژوهش از نظر کاربردی و از نظر روش ماهیت جزء روش های تحقیق توصیفی تحلیلی است. اطلاعات و داده های مورد نیاز از طریق روش کتابخانه ای استفاده شده است.

واژگان کلیدی: کاربرد، هوش مصنوعی، اهمیت، امنیت IT.

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۹، بهار ۱۴۰۲، ص ۲۲- ۱۴

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

با توجه به پیشرفت هایی که در صنعت مهندسی برق، رایانه و مخابرات پدید آمده است و همچنین وقوع حوادث، جنگ، حملات نظامی کشور های مهاجم و نیز تهدیدات سایبری، لزوم بهره برداری از انرژی الکتریکی استفاده کرد. شبکه های عصبی مصنوعی ایده ای برای پردازش اطلاعات است. این سیستم از شمار زیادی عناصر پردازشی فوق اعاده به نام نورون ها (neurons) تشکیل شده است(۶). در سال های اخیر با پیشرفت هایی که در زمینه هوش مصنوعی صورت گرفته، روش های محاسباتی مبتنی بر یادگیری در طیف وسیعی از کاربرد ها به کار گرفته شده است. هوش مصنوعی شامل تعدادی تکنیک مانند بهینه سازی ازدحام ذرات (PSO)، عصبی شبکه (NN) می‌باشد (۴). هوش مصنوعی شامل کمک در بهبود طول عمرشبکه می باشد. همچنین ممکن است برای مسیر یابی بهتر استفاده شود. پیشرفت در تکنولوژی اجازه می دهد تا کامپیوتر ها از راه دور مدیریت شود (۳). سازمان ها با مسائل اطلاعات محافظت شده، در دسترس و قابل اطمینان رو به رو می شوند. برخی کاربران برای دسترسی به این اطلاعات محرمانه از کدهای مخرب کمک می گیرند. انواع مختلفی از کدهای مخرب که روزانه رویکرد دسترسی بی اجازه به محتوا را دارند، وسیع تر و رایج تر می شود. بنابراین برای گذر این مسائل کمپانی های افزایش بودجه از طریق توسعه سیستم های شناسایی دسترسی غیر مجاز که بر مبنای تکنولوژی های هوش مصنوعی است را در پیش می گیرند (۱). سیستم های تشخیص نفوذ شبکه (NIDS) در زیر ساخت های محاسباتی مدرن برای کمک به نظارت و شناسایی ترافیک شبکه های نامطلوب و مخرب مانند دسترسی سیستم های پیکربندی ضعیف ضروری هستند. هوش مصنوعی (Intelligence Artificial) یا AI فناوری شاخه ای در علوم کامپیوتر است که به مطالعه و توسعه نرم‌افزار و دستگاه‌های هوشمند می پردازد (۲). هوش مصنوعی به سیستم‌هایی گفته می‌شود که می توانند واکنش هایی مشابه رفتارهای هوشمند انسانی از جمله درک شرایط پیچیده و شبیه سازی فرایند های تفکری را داشته باشد. شبکه های عصبی مصنوعی ابزاری محاسبتی اند که رفتاری شبیه به رفتار شبکه های عصبی طبیعی دارند. در سال های اخیر انواع مختلفی از شبکه های عصبی ارائه شده اند که در اکثر علوم کاربردی خاص خود را یافته اند. در یک تعریف ساده شبکه های عصبی مصنوعی متشکل از نرون های متصل به هم هستند (۵). شبکه های عصبی مصنوعی را می توان یک تکنولوژی رایانشی نرم دانست که در سطح زیادی موردمطالعه قرارگرفته و در طی دو دهه ی اخیر نیز کاربردهای زیادی از آن پدید آمده است. رایج ترین کاربردهای شبکه های عصبی را می توان در حل مسائل تشخیص الگو، تحلیل داده ای، کنترل و خوشه بندی دانست. شبکه های عصبی مصنوعی دارای ویژگی های زیادی منجمله سرعت پردازشی بالا و توانایی در یادگیری و به دست آوردن جواب یک مسئله از طریق یادگیری یک مجموعه داده ای می باشند (۱۰). هدف این مقاله بررسی کاربرد هوش مصنوعی و امنیت آن در امنیت IT می باشد.

هوش مصنوعی

بعضی از مبشرین هوش مصنوعی ادعا می‌کنند که این نیروی جدید فناورانه می‌تواند تمام آنچه دیگران به ظاهر بی‌ربط می‌دانند را ارائه کند، با توجه به مقیاس تغییر، خطر و فرصتی که می‌توانست برای امنیت IT بیاورد. این هنر تاریک جدید که فناوری ظاهرا جادویی را به صورت افسونگری پیشنهاد می‌کند قطعا پتانسیل این را دارد که جهان ما را تغییر دهد و - بسته به اینکه چه کسی را باور کنید - ممکن است زندگی را کمی بهتر کند، منجر به تحول کلی جامعه شود یا به خود بشریت پایان دهد (۱۲). هوش مصنوعی پتانسیل مختل کردن تمام بخش‌های صنعت را دارد – این زمینه از علوم کامپیوتر روی ایجاد ابزار نرم‌افزاری هوشمندی متمرکز است که توانایی‌های ذهنی حیاتی بشر را تکرار می‌کنند. بازه‌ی کاربردها شامل این موارد است: شناخت کلام، ترجمه‌ی زبان، ادراک بصری، یادگیری، استدلال، استنباط، ایجاد استراتژی، طرح‌ریزی، تصمیم گیری و درک مستقیم. به عنوان نتیجه‌ای از یک نسل جدید از فناوری‌های مخرب و هوش مصنوعی ما در حال ورود به انقلاب صنعتی چهارم هستیم (۸). سه انقلاب قبل به ما ماشینی کردن بر مبنای بخار، برق رسانی و تولید جرم، سپس الکترونیک، فناوری اطلاعات و فرایند مکانیزه کردن کارها را عرضه کرد. این دوره‌ی جدید چهارم با دستگاه‌های هوشمندش با بهبود پتانسیل و همگرایی چند زمینه‌ی علمی و فناوری تقویت شده‌است، مانند کلان داده، هوش مصنوعی، اینترنت اشیاء (IoT)، سخت افزار فوق محاسباتی، ارتباطات مفرط، رایانش ابری، ارزهای دیجیتال، بلاکچین سیستم‌های دفتر حساب توزیع شده و محاسبات همراه. نتایج میان

ISSN: 2745-3673
http://www.Rcsj.ir

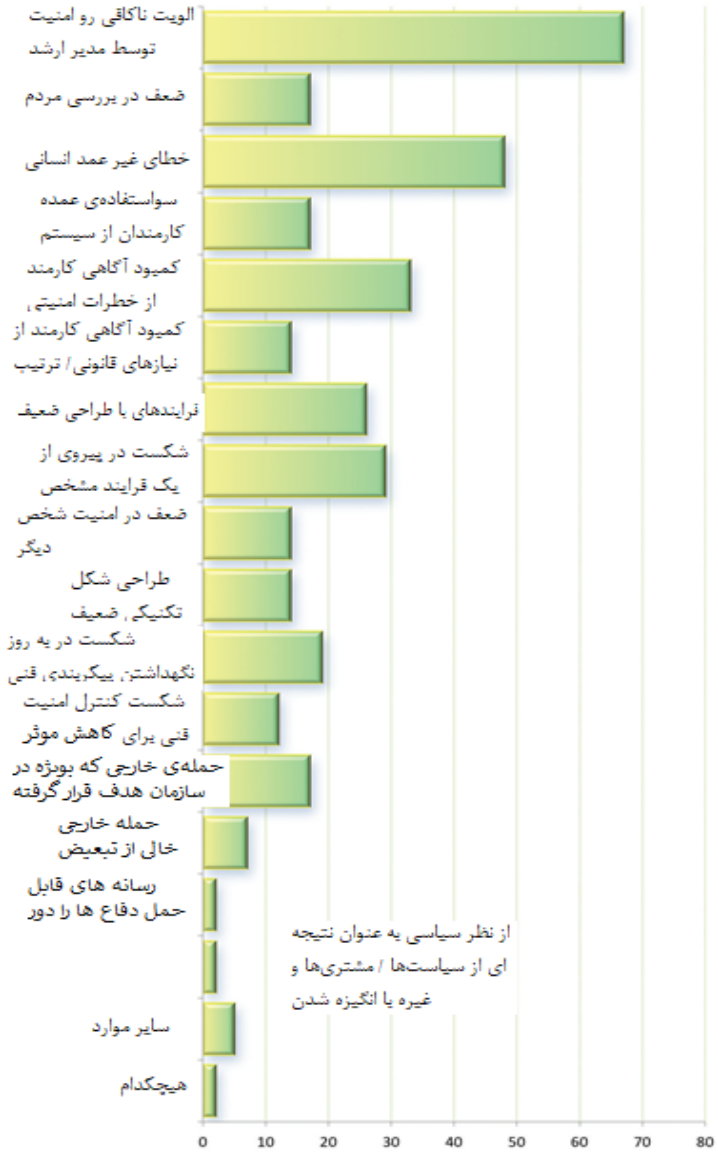
مدت و طولانی مدت این فناوری‌های نمایی همگرا برای افراد، جامعه، تجارت، دولت و امنیت فناوری اطلاعات اصلا واضح نیستند (۹). سرعت پیشرفت هوش مصنوعی رو به افزایش است و این حتی برای کسانی که در این بخش هستند هم حیرت انگیز است. در ماه مارس سال ۲۰۱۶، سیستم دیپمایند آلفاگو گوگل[1] با نشان دادن سرعت پیشرفت در ماشین یادگیری، قهرمان Go جهان را شکست داد- فناوری هوش مصنوعی مرکزی. در بازی تخته‌ای Go بیش از ۵۶۰ میلیون حرکت امکان پذیر است- نمی‌توانید به سیستم تمام قوانین و جایگشت‌ها را آموزش دهید (۷). در عوض، آلفاگو به یک الگوریتم ماشین یادگیری مجهز شده بود که با استفاده از آن می‌توانست قوانین و حرکات ممکن را با مشاهده‌ی هزاران بازی استنباط کند. همین فناوری امروزه می‌تواند در امنیت فناوری اطلاعات در برنامه‌های کاربردی از شناسایی تهدیدات خارجی و جلوگیری از آن تا مشخص کردن ماده متشکله‌های رفتارهای غیرقانونی بالقوه در میان کارمندان استفاده شود (۱۵).

وضعیت امنیت فعلی

در سال ۲۰۱۵ در آمریکا، مرکز منابع سرقت هویت به این نکته اشاره کرد که تقریبا ۱۸۰ میلیون سوابق شخصی در معرض نقض داده‌ها قرار گرفتند و گزارش بررسی PwC مشخص کرد که ۷۹٪ سازمان‌های پاسخگوی آمریکا حداقل یک حادثه‌ی امنیتی را تجربه کرده‌اند‌در سال ۲۰۱۵ در ایالات متحده، مرکز منابع سرقت هویت خاطرنشان کرد که تقریباً ۱۸۰ میلیون پرونده شخصی در معرض نقض داده‌ها بوده‌است و گزارش بررسی PwC نشان می‌دهد که ۷۹٪ سازمان‌های پاسخ دهنده آمریکا حداقل یک واقعه امنیتی را تجربه کرده‌اند (۱۳). پژوهش‌های صنعتی نشان می‌دهد که وقتی هکرها با گذشت چند دقیقه از شناخته شدن آن‌ها از آسیب پذیری‌ها بهره‌برداری می‌کنند، شرکت‌ها به سختی ۱۴۶ روز برای اصلاح آسیب پذیری‌های بحرانی وقت می‌گذارند. از آنجا که میانگین قیمت تخمین زده شده برای نقض داده‌ها ۴ میلیون دلار است، امروزه و در آینده نگرانی رو به افزایش در این مورد وجود دارد که شرکت‌ها چگونه می‌توانند این یورش همیشگی از حملات به هرصورت دزدکی، سریعتر و از روی دشمنی را تحمل کنند. همانگونه که به نظر می‌رسد، بسیاری از واحدهای اقتصادی بیشتر از حفظ امنیت روی واکنش به نقض امنیت تمرکز می‌کنند و روش کار حاضر برای امنیت شبکه اغلب به جای شناسایی تهدیدهای جدید و رو به تکامل بیشتر به دنبال براوردن استانداردها هستند(۱۸). نتیجه‌اش یک بازی بدون برد است که می‌تواند شرکت‌ها را در آینده در هم بشکند مگر اینکه آنها مایل باشند طرز فکر، فناوری و روش‌های مورد استفاده‌ی هکرها را بپذیرند و خودشان را با آن‌ها وفق دهند (۲۰). همچنین یک شک کوچک در این مورد وجود دارد که هکرها در حال توسعه‌ی ابزارهای هوش مصنوعی هستند یا به زودی خواهند بود تا دفعات، مقیاس، نقص و مهارت حملاتشان را افزایش دهند (۱۶). در این عصر دیجیتال سازمان‌ها هم به صورت درونی از طریق فرایندهای خودشان و هم از خارج با مشتری‌ها، فروشنده‌ها و شرکایشان مقادیر نامحدودی از داده‌ها را ایجاد می‌کنند. هیچ بشری قادر به تحلیل تمام آن داده‌ها نیست تا برای نقض بالقوه‌ی امنیتی پایش کند- سیستم‌های ما به سادگی بسیار گسترده، مملو از داده‌ها و بی‌روح شده‌اند. با این حال، هنگامی که با ابزارهای مدیریت کلان داده ترکیب می‌شوند، هوش مصنوعی حتی در فشرده‌سازی مقادیر زیادی از داده‌ها و بکار بردن الگوها و بیرون کشیدن ناهنجاری‌ها موثرتر می‌شود. در حقیقت، بیشتر سیستم‌های هوشمند، هرچه بیشتر اطلاعات تغذیه کنند باهوش‌تر می‌شوند (۱۱).

[1] Google DeepMind’s AlphaGo system

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۱: عواملی که موجب حوادث امنیتی می‌شوند. منبع: بررسی نقض اطلاعات امنیتی PwC ۲۰۱۵

شکل ۲: تعداد نقض ها در سال ۲۰۱۵، با بخش. منبع: مرکز منابع سرقت هویت

ISSN: 2745-3673
http://www.Rcsj.ir

پتانسیل آینده

یکی از بزرگترین منافع بالقوه‌ی امنیتی مربوط به هوش مصنوعی در شناسایی تهدیدات داخلی نهفته است. یک سیستم هوش‌مصنوعی را تصور کنید که تمام مدت رفت و آمد تمام کارمندان را به دفاتر مرکزی شرکت از طریق زیست‌سنجی و اطلاعات ورود رصد می‌کند. این سیستم برای مثال می‌داند که CFO به شکل معمول هر روز ساعت ۱۲ ظهر از ابر خارج می‌شود و به ورزشگاه شرکت سری می‌زند، او به طور میانگین ۴۵ دقیقه را در آنجا می‌گذراند (۲۲). یک روز یک ناهنجاری را کشف کرد- CFO در ساعت ۱۲:۲۰ بعدظهر به ابر وارد شد. این سیستم هوشمند به اندازه‌ی کافی باهوش است که بتواند موقعیت را با این ورود غیرمنتظره مقایسه کند- با توجه به داده‌هایش، صورت CFO آخرین بار هنگام ورود به ورزشگاه اسکن شده بود و خروجش از باشگاه دیده نشده بود، اما این ورود به ابر از دفتر کار او سرچشمه گرفته بود. این هوش مصنوعی این ناهنجاری را تشخیص می‌دهد، بین مغایرت ورود و موقعیت‌های CFO ارتباط ایجاد می‌کند، دسترسی ابری را برای حساب CFO خاموش می‌کند و اقدامات دفاعی را در مقابل حملات بالقوه‌ی سایبری آغاز می‌کند (۲۴). این سیستم همچنین به CFO اعلام خطر می‌کند و در مدت چند ثانیه این مشکل با اولویت بالا را برای امنیت- سایبری بشر بزرگ نمایی می‌کند. داده‌های مهم شرکت و پرونده‌های مالی به لطف امنیت هوشمند ایمن هستند (۲۳). تصور کنید همانطور که این سیستم هوشمند به یادگیری و پیش بینی رفتار صدها یا هزاران کارمند در میان سازمان ادامه می‌دهد چطور توانایی‌هایش رشد خواهند کرد- به سازمان کمک می‌کند که نقض‌های امنیتی مشابه را پایش و پیش بینی کند. آنسوی رفتار کارمند، این کاربرد امنیتی هوشمند نیز سیستم ورود شرکت را رصد می‌کند و یاد می‌گیرد که آن‌ها چطور تعامل دارند (۲۱). زمان افزوده شدن اطلاعات مشتری را در پایگاه داده‌ی شرکت کشف می‌کند، این اطلاعات به صورت خودکار با نرم‌افزار حسابداری انتخاب شده است و یک فاکتور به صورت میانگین در ۷.۵ ثانیه تولید شده است. هرگونه انحراف خارج از رفتار عادی در ۰.۲۵ ثانیه این هوش مصنوعی را راه‌اندازی می‌کند تا هر پیوندی را در فرایند بررسی کند و علت را رفع کند. در این مورد، بر پایه‌ی آنچه کشف می‌کند (یک تاخیر غیرمنطقی در این سیستم)، امنیت هوشمند به طور صحیح رویداد را غیر تهدیدآمیز و کم خطر اولویت بندی می‌کند، اما به پایش خود برای تاخیرهای مشابه ادامه می‌دهد و سیستم هشدار برای حفظ این موضوع نگهداری می‌شود (۲۰).

«این دوران جدید با همگرایی زمینه‌های علمی و فناورانه تقویت شده است، مانند کلان داده، هوش مصنوعی، اینترنت اشیا (IoT)، سخت‌افزار ابر محاسباتی، ارتباطات مفرد، محاسبات ابری، ارزهای دیجیتال، بلاکچین سیستم‌های دفتر حساب توزیع شده و محاسبات سیار»

اکنون اجازه دهید این سناریو را یک مرحله جلوتر ببریم- تصور کنید که نه تنهااین سیستم هوشمند رفتار صدها کارمند و شبکه‌های ورودی شرکت را یاد گرفته است، بلکه همچنین می‌تواند به صورت پیوسته از حملات سایبری خارجی نیز یاد بگیرد. هرچقدر به این هوش مصنوعی حملات سایبری بیشتری وارد شود، می‌تواند داده‌های بیشتری را تجزیه کنند و مانند یک تفکر، یعنی اینکه یک سرباز عاقل برج و بارویش را از طریق نبردهای متعدد اداره کرده‌است، برای حملات آینده بهتر آماده می‌شود و تعلیم می‌بینند. کد دشمن بر اساس تجربه‌ی گذشته و مواجهه‌ی پیشین با الگوهای مرتبط رفتار حمله را کاملا جدید تشخیص خواهد داد (۱۷). این سیستم همانطور که برای حل کردن کد جدید دشمن کار می‌کند حالت دفاعی هم خواهد ساخت: و همانطور که کد هوشمند دشمن قصد می‌کند که با حالات دفاعی جدید تطبیق پیدا کند، امنیت هوشمند به طور پیوسته روش‌های جدیدی را برای تلاقی و نابودی این متجاوز بدست می‌آورد (۲۶).

«هرچقدر به این هوش مصنوعی حملات سایبری بیشتری شود، می‌تواند داده‌های بیشتری را تجزیه کنند و مانند یک تفکر، یعنی اینکه یک سرباز عاقل برج و بارویش را از طریق نبردهای متعدد اداره کرده‌است، برای حملات آینده بهتر آماده می‌شود و تعلیم می‌بینند.»

این سیستم امنیتی بالقوه هوشمند در آینده‌ی نزدیک است- که از داخل و بیرون کاملا یکپارچه است، نسبت به کسب و کار روزانه غیر تهاجمی است و همیشه هوشیار و آماده‌ی دفاع است. این غایت نگهبانی دیجیتالی خواهد بود- که به شکل امیدوار کننده‌ای به سرعت حملات یاد می‌گیرد و خود را وفق می‌دهد (۲۵).

ISSN: 2745-3673
http://www.Rcsj.ir

رویکرد سازمان‌ها

همانطور که جنگ با میله‌ها سرانجام به جمگ با سلاح‌های هسته‌ای تبدیل شد، نبرد هوش مصنوعی بین سازمان‌ها و هکرها هم همانطور خواهد بود. برتری جویی مداوم در امنیت هوشمند معیار خواهد شد، شاید تا جایی که حتی توسعه دهندگان هم نتوانند کار واقعی یادگیری ثابت و الگوریتم‌های ثابت یادگیری و کامل کردن امنیت‌شان را رمزگشایی کنند (۲۹). همانقدر که تمام این‌ها پیچیده و گران قیمت به نظر می‌رسند، آیا شرکت‌ها بویژه سازمان‌های کوچکتر، در آینده قادر خواهند بود بدون هوش مصنوعی پا بر جا بمانند؟ هرچه سهام افزایش پیدا می‌کند و شکست‌ها بزرگتر جلوه می‌کنند، تهدیدهای همیشه درحال تحول هوشمند ممکن است همکاری را بین چند شرکت بیشتر تشویق کنند. سازمان‌های کوچکتر می‌توانند با هم تحت یک سیستم امنیتی هوشمند متحد شوند، هزینه و پشتیبانی را بین چند پرداخت کننده پخش کنند، درحالیکه اجرا کنندگان بزرگتر با قدرت فناورانه و مالی قویتر برای دستیابی به امنیت هوشمندشان ممکن است درواقع اطلاعات حیاتی را روی حملات سایبری معامله کنند- یا ترجیحا، هوش مصنوعی آن‌ها می‌تواند اطلاعات را روی حملات سایبری معامله کند و از یکدیگر یاد بگیرند (۲۷).

«درحالیکه سیستم هوشمند توسط چند امنیت سایبری هوشمند پشتیبانی می‌شود، تمام سیستم ساده‌ی امنیت در دستان کارمندان است، که بطور گسترده شانس نقض امنیت را زیاد می‌کند»

متناوبا، شرکت‌ها می‌توانند آنقدر درهم بشکنند که به سادگی راه‌حل‌های غیر هوشمند ساده و از نظر فناوری ارزانتر «جستجوی فراگیر» را برای شمارش هک‌های هوشمند پیچیده‌ی رو به افزایش انتخاب کنند. راه‌حل ساده یا غیرهوشمند ممکن است مستلزم تست‌ها و رمزهای بیشتری برای دستگاه‌ها و حساب‌های کاربری باشد، یا شاید دستگاه‌های با امنیت پیشرفته که هر دو هفته تغییر کنند. درحالیکه افزودن ۵ لایه رمز پیچیده برای هر ورود یا چرخش پیوسته از طریق تلفن‌های هوشمند می‌تواند امنیت شرکت را حفظ کند، افزایش سربار، محروم سازی کارمند و اتلاف زمان با اقدامات دشوار امنیتی ایده‌آل دیده نخواهد شد و می‌تواند مانع اعتبار این شرکت شود- که ممکن است آن را نسبت به حمله حساس‌تر کند (۱۶). یک سیستم هوشمند آهسته امنیت را پایش می‌کند و کارمندان را به تمرکز بر کارشان قادر می‌سازد، در حالیکه این راه‌حل غیرهوشمند ساده بار امنیتی غیر ضروری را روی کارمندان می‌گذارد- آن‌ها مسئول نگهداشتن آن پنج رمز و تغییر دستگاه‌ها روی یک پایگاه به صورت دوبار در هفته خواهند بود (۲۸). سیستم هوشمند توسط چند امنیت سایبری هوشمند پشتیبانی می‌شود در حالیکه سیستم ساده‌ی امنیتی کاملا در دست تمام کارمندان است، این به طور گسترده شانس نقض ایمنی را چند برابر می‌کند. در آینده، این راه‌حل ساده‌ی غیر هوشمند ممکن است به یک راهبرد تدافعی برای بقا تبدیل شود تا اینکه یک نبرد تدافعی سازگار از یک کسب و کار پررونق پیشرو باشد (۳۱).

نقش انسان‌ها

البته، در این مرحله یک سوال طبیعی پیش می‌آید: اگر هوش مصنوعی سریعتر و هوشمندتر باشد و به طور پیوسته خود را با کارش تطبیق دهد، چرا با امنیت سایبری انسان به دردسر بیفتد؟» امروزه، امنیت هوشمند هنوز باید از انسان‌ها یاد بگیرد و هرچند ممکن است یک روز به این مرحله برسد که دیگر نیازی به درگیری متخصص نداشته باشد، آن روز حداقل چند سال در مسیر باقی می‌ماند. علاوه بر این، بسته به اینکه چقدر اشتباه بشر و شهود در امنیت را در نظر بگیریم، ممکن است آن روز هرگز وارد مسیر نشود. سیستم‌های امنیتی هوشمند در حال حاضر به انسان‌ها نیاز دارند تا الگوریتم‌های آغازگرشان را بنویسند و داده‌ی لازم را فراهم کنند، تعلیم بدهند و بازخورد بدهند تا یادگیرندگانشان را راهنمایی کنند (۳۲). انسان‌ها در حال حاضر بخش ضروری گسترش هوش مصنوعی هستند و همانطور که امنیت هوشمند بهتر این مرحله‌ی پیدایش را کامل می‌کند، این نقش برای انسان‌ها در هوش مصنوعی به همان میزان کامل خواهد شد. وقتی سازمان‌ها به شکل فزاینده‌ای فرایندها را دیجیتالی می‌کنند، مقادیر شگفت‌انگیز باهوش داده‌های حساس، نقش معماران بشری و متفکران سیستم‌های امنیت هوشمند اهمیت جدیدی خواهد یافت. هرگز این میزان داده به راحتی در دسترس حملات نبوده است و حتی حملات کوچکی که داده‌های به ظاهر بی‌ضرر را جمع می‌کنند می‌توانند به نقض فاجعه‌آمیز امنیت بی‌افزاید. توسعه‌دهندگان امنیت هوشمند به نگهبانان

ISSN: 2745-3673
http://www.Rcsj.ir

سلاح‌های هسته‌ای در اهمیت وابسته خواهند شد – افراد معتمدی که آزمایش‌های زمینه‌ای گسترده و آموزش گسترده، بررسی و اعتبارگذاری را پشت سر گذاشته‌اند. آن‌ها نه تنها امنیت هوشمند خواهند ساخت، بلکه اشتباه و راهنمایی گسترده در این فرایند آموزش را فراهم خواهند کرد و خط کاملی از دفاع امنیت سایبری خواهند بود. امنیت هوشمند فراتر از توانایی‌های انسان خواهد رفت، سازمان‌ها و متخصصین امنیت سایبری را از وظیفه‌ی غیر ممکن مراقبت ثابت رها خواهد کرد، به آن‌ها اجازه می‌دهد از حملات آینده بدون ایجاد وقفه در جریان کار روزانه جلوگیری کنند. سیستم امنیت هوشمند فردا یاد خواهد گرفت، خودش را اصلاح خواهد کرد و در پشت صحنه به صورت محتاطانه اجرا خواهد شد- پایش هوشمندانه، اولویت بندی و نابودی حملات: تکامل همیشگی سلاح ظریف ریز در اسلحه خانه‌ی امنیت سایبری (۳۰).

نتیجه گیری

مسائل یا اهداف اصلی در تحقیقات هوش مصنوعی به منطق، دانش، طراحی، یادگیری، ارتباطات، درک و توانایی حرکت دادن یا استفاده از اشیاء مربوط می شود. هوش مصنوعی یا هوش مصنوعی قوی هنوز یکی از اهداف بلند مدت است. روش هایی که در حاظر محبوبیت دارند، عبارتند از روش های آماری، هوش محاسباتی و هوش‌مصنوعی سمبولیک سنتی. درهوش مصنوعی از ابزارهای متنوعی استفاده شده که شامل نسخه هایی از بهینه سازی تحقیق و ریاضیات، منطق، روش های مبتنی بر احتمالات و اقتصاد و بسیاری موارد دیگر می‌شود. این رشته مبتنی بر این ادعا است که توانایی اصلی انسان، هوش را می توان به گونه‌ای دقیق توصیف کرد که دستگاه‌ها هم قادر به شبیه‌سازی آن باشند. این ادعا مسائل فلسفی را درباره ماهیت ذهن و مشکل اخلاقی خلق موجودات مصنوعی دوباره زنده می کند که از دیرباز در اسطوره ها، افسانه ها و فلسفه به آنها پرداخت شده است. هوش مصنوعی همواره با خوش‌بینی همراه بوده اما شکست هایی را نیز تجربه کرده است. امروزه هوش مصنوعی به بخشی ضروری از صنعت فناوری و بسیاری از دشوارترین مسائل علوم کامپیوتر تبدیل شده است. با توجه به اهمیت شبکه قدرت در امنیت ملی که یکی از مهمترین نگرانی های متولیان سامانه قدرت است، استفاده ازهوش مصنوعی توزیع شده در زیر ساخت های کنترل ناحیه گسترده باعث ایجاد طراحی انعطاف پذیر برای کنترل شبکه قدرت شده است. افزایش ارتباطات بیسیم و استفاده از آن در مناطق مختلف باعث رشد بسیار شبکه های رایانه ای بیسیم شده است. شبکه های سیار به علت دسترسی آسان تر و بهتر بیشتر مورد توجه قرارگرفته اندکه از موارد مهم آن شبکه ها، مسیریابی و برقراری ارتباط بین مبدا و مقصد است. شبکه های عصبی در بسیاری از زمینه های تحقیقاتی از جمله مهندسی برق، رایانه، سازه و بیولوژی به کارگرفته شده است. سیستم تشخیص تهاجم، یک ابزار موثر برای جلوگیری از دست‌یابی غیر مجاز به منابع شبکه است که یک سیستم تشخیص تهاجم خوب باید تشخیص بالا و میزان خطای پایین و کم باشد.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[۱] اسماعیلی و همکاران، (۱۴۰۰)، مروری بر کاربردهای هوش مصنوعی و واقعیت مجازی در آموزش، فصلنامه مطالعات اندازه گیری و ارزشیابی آموزشی، دوره ۱۱، شماره ۳۶.

[۲] حسنی آهنگر و همکاران، (۱۳۹۰)، یک روش مسیریابی در شبکه های سیار موردی با استفاده از فن های هوش مصنوعی توزیع شده، مجله علمی و پژوهشی، علوم و فناوری های پدافند غیر عامل، سال دوم ، شماره ۴.

[۳] خانزاده، محمد حسین و نباتی راد، محمد حسین، (۱۳۹۴)، ساختار کنترلی مبتنی بر هوش مصنوعی توزیع شده به منظور بهبود پایداری شبکه قدرت در مواقع بحران، علمی و پژوهشی، علوم و فناوری های پدافند نوین، جلد ۶، شماره ۴.

[۴] صفری، احرام و انصاری، علی اصغر، (۱۴۰۱)، شناسایی و رتبه بندی عوامل موثر بر پذیرش هوش مصنوعی در بخش دولتی و خصوصی، فصلنامه مطالعات مدیریت کسب و کار هوشمند، سال یازدهم، شماره ۴۱.

[۵] طیبی قصبه و همکاران، (۱۳۹۳)، مهندسی برنامه های کاربردی هوش مصنوعی، چارچوب بهینه برای تشخیص نفوذ در شبکه های کامپیوتری، اولین همایش ملی پژوهش های مهندسی رایانه.

[۶] عزیز پوران، زهرا و مرادی، علیرضا، (۱۴۰۱)، کاربرد هوش مصنوعی در مدیریت، دومین کنفرانس بین‌المللی مهندسی و علوم کامپیوتر.

[۷] فرج، شعیب و امینی، سرحد، (۱۳۹۵)، هوش مصنوعی در شبکه های کامپیوتری (شبکه عصبی)، سومین همایش ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران.

[۸] ناصری پبدنی، علی، (۱۳۹۹)، هوش مصنوعی در مهندسی کامپیوتر، کنفرانس بین المللی پژوهش های نوین در مهندسی برق، کامپیوتر، مکانیک و مکاترونیک در ایران و جهان اسلام.

[9] A. Sadegheih," Artificial Intelligences in the Topological Configuration of the Network", 18 International power system conference, 98-E-DTC-215.

[10] Alsheibani, S., Cheung, Y., & Messom, C. (2018). Artificial Intelligence Adoption: AI-readiness at Firm-Level. In PACIS (p. 37).

[11] Alsheibani, S. A., Cheung, D., & Messom, D. (2019). Factors inhibiting the adoption of artificial intelligence at organizational-level: A preliminary investigation. https://researchmgt. monash. edu/ws/portalfiles/portal/287736273/287674072_oa. Pdf.

[12] Alex Shenfield, David Day, Aladdin Ayesh," Intelligent intrusion detection systems using artificial neural networks", The Korean Institute of Communications and Information Sciences (KICS). Publishing Services by Elsevier B.V. This is an open access article under the CC BY-NC-ND license ,2018 (http://creativecommons.org/licenses/by-nc-nd/4.0/).

[13] Bakshi, S. K., Lin, S. R., Ting, D. S. W., Chiang, M. F., & Chodosh, J. (2020). The era of artificial intelligence and virtual reality: transforming surgical education in ophthalmology. British Journal of Ophthalmology.

[14] Chang, J., & Lu, X. (2019). The Study on Students' Participation in Personalized Learning Under the Background of Artificial Intelligence. Paper presented at the 2019 10 th International Conference on Information Technology in Medicine and Education (ITME).

[15] Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. IEEE Access, 8, 76264-75278.

[16] Chatterjee, S., 2020. AI strategy of India: policy framework, adoption challenges and actions for government. Transforming Government: People, Process and Policy, 14(5), pp. 757-775. https://doi. org/ 10. 1108/TG-05-2019-0031.

[17] Copeland, Jack, Artificial Intelligence: A Philosophical Introduction, New York: Blackwell (1993).

[18] 18 - Desouza, Kevin. Managing Knowledge With Artificial Intelligence, London: Westport, (2002).

[19] Dasgupta, A., Wendler, S. (2019). AI Adoption Strategies. University of oxford. https://www. ctga. ox. ac. uk/files/aiadoptionstrategiesmarch2019pdf.

ISSN: 2745-3673
http://www.Rcsj.ir

[20] ‘2015 Information security breaches survey’. PwC. Accessed Apr 2017. www.pwc.co.uk/services/audit-assur ance/insights/2015-information security-breaches-survey.html.

[21] Fernando Luiz Koch, Carlos Becker Westphall,” Decentralized Network Management Using Distributed Artificial Intelligence “,Journal of Network and Systems Management, Vol. 9, No. 4, December 2001.

[22] Hradesh Kumar, Pradeep Kumar Singh,” Comparison and Analysis on Artificial Intelligence Based Data Aggregation Techniques in Wireless Sensor Networks”, International Conference on Computational Intelligence and Data Science (ICCIDS 2018).

[23] Fanyu Bu, Xin Wang, Bo Gao,” A Multi-Projection Deep Computation Model for Smart Data in Internet of Things “,Internet of Things, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.09.060.

[24] Hadi Salehi, Saptarshi Das, Subir Biswas, Rigoberto Burgueño,” Data mining methodology employing artificial intelligence and a probabilistic approach for energy-efficient structural health monitoring with noisy and delayed signals”, Expert Systems With Applications 135 (2019) 259–273, ELSEVIRE.

[25] Hradesh Kumar and Pradeep Kumar Singh,” Comparison and Analysis on Artificial Intelligence Based Data Aggregation Techniques in Wireless Sensor Networks”, International Conference on Computational Intelligence and Data Science (ICCIDS 2018). ELSEVIRE.

[26] Haugeland, John. Artificial Intelligence; The Very Idea, Massachusetts, The MIT Press (1985).

[27] I dentity Theft Resource Centre Breach Report hits near record high in 2015’. Identity Theft Resource Centre, 25 Jan 2016. Accessed Apr 2017. www.idtheftcentre.org/ITRC Surveys-Studies/2015databreaches. html.

[28] Koushal Kumar, Gour Sundar Mitra Thakur,” Advanced Applications of Neural Networks and Artificial Intelligence: A Review “,I.J. Information Technology and Computer Science, 2012, 6, 57-68 Published Online June 2012 in MECS (http://www.mecs-press.org/).

[29] MIN-CHUNYU,” MULTI-CRITERIA ABC ANALYSIS USING ARTIFICIAL-INTELLIGENCE-BASED CLASSIFICATION TECHNIQUES”, EXPERT SYSTEMS WITH APPLICATIONS, VOLUME 38, ISSUE 4, APRIL 2011, PAGES 3416–3421, ELSEVIER - SCIENCE DIRECT.

[30] Searl, John, Minds, Brains and Science, London: Penguin, (1989).

[31] Stillings, Neil & Weisler, Steven. Cognitive Science: An Introduction, NewYork: Massachusetts Institute of Technology, (1995).

[32] Takeshi Okamoto, “An artifi cial intelligence membrane to detect network intrusion”, Artif Life Robotics (2011) 16:44–47 © ISAROB 2011, DOI 10.1007/s10015-011-0880-5.