بررسی نقش هوش مصنوعی در امنیت سایبری

فائقه اختری

گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آیت‌الله العظمی بروجردی، بروجرد، لرستان

سید منصور شهیدی

گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آیت‌الله العظمی بروجردی، بروجرد، لرستان

چکیده

چشم‌انداز امنیت سایبری به دلیل پیشرفت هوش مصنوعی به سرعت در حال تغییر است. هدف از این مقاله بررسی نقش هوش مصنوعی در تقویت امنیت سایبری در برابر تهدیدات سایبری پیچیده می‌باشد. نقش هوش مصنوعی در امنیت سایبری شبیه یک شمشیر دولبه است. از یک طرف، ابزارهای پیشرفته‌ای را برای افزایش اقدامات امنیتی، شناسایی موثرتر تهدیدات و پاسخ سریع به حملات ارائه می‌دهد. این قابلیت‌ها ناشی از توانایی هوش مصنوعی برای تجزیه‌وتحلیل سریع حجم زیادی از داده‌ها و شناسایی الگوهایی است که ممکن است نشان‌دهنده‌ی نقض امنیتی باشد. از سوی دیگر، هوش مصنوعی با ارائه‌ی روش‌های پیچیده برای اجرای حملات به مجرمان سایبری قدرت می‌دهد. یادگیری ماشینی و یادگیری عمیق حملات سایبری پیچیده‌تر و آسیب‌رسان‌تر را تسهیل می‌کنند که سریع‌تر، هدفمندتر و مخرب‌تر هستند. انتظار می‌رود که تأثیر هوش مصنوعی بر امنیت سایبری، چشم‌انداز تهدید را گسترش داده، تهدیدات جدیدی را معرفی نموده و ماهیت معمولی تهدیدات را تغییر دهد. چالش‌های مهمی مانند حفظ حریم خصوصی داده‌ها، آموزش مداوم مدل‌های هوش مصنوعی، خطرات دستکاری و استانداردهای اخلاقی بررسی می‌شوند. چشم‌انداز در حال تحول تهدیدات سایبری، مستلزم پیشرفت مداوم در استراتژی های دفاعی است. در حالیکه هوش مصنوعی کاربردهای گسترده‌ای در سراسر فناوری اطلاعات دارد، ادغام آن در امنیت سایبری پیشرفت جدیدی است. توسعه‌ی دستورالعمل‌هایی که استفاده‌ی مسئولانه و مؤثر از هوش مصنوعی در امنیت سایبری را تضمین می‌کند، با هدف افزایش یکپارچگی و حریم خصوصی سیستم بدون به خطر انداختن امنیت، تسهیل می‌گردد.

واژگان کلیدی: هوش مصنوعی، امنیت سایبری، یادگیری ماشینی

مقدمه

هوش مصنوعی (AI) را می‌توان به عنوان سیستمی توصیف کرد که محیط اطراف خود را تشخیص می‌دهد و فعالیت‌هایی را انجام می‌دهد که احتمال موفقیت‌آمیز بودن هدف را افزایش می‌دهد. هوش مصنوعی تلفیقی از هوش فیزیکی و فناوری است که می‌توان از آن برای به دست آوردن نتایج دلخواه استفاده کرد. این مفهوم ابزاری را برای حل چالش‌های پیچیده و سخت در یک سیستم کامپیوتری فراهم می‌کند. کنترل‌های امنیت اطلاعات بهبودیافته با هوش مصنوعی تعبیه‌شده جهت محافظت از سازمان‌ها در برابر عوامل تهدید بتدریج استفاده می‌شوند. انگیزه‌ی هوش مصنوعی، تسهیل توانایی سیستم‌های رایانه‌ای بمنظور جعل هویت قابلیت‌های تفکر شناختی انسان‌ها به منظور تکرار رفتار آنها جهت حل چالش‌ها، سریع‌تر و مؤثرتر از آنچه که افراد می‌توانند انجام دهند، می‌باشد. فعالیت‌های متعددی از جمله استراتژی‌سازی، مهاجرت، برقراری ارتباط، شناسایی هدف و نویز، فعالیت‌های خلاقانه و عملیات شرکت را می‌توان بوسیله‌ی هوش مصنوعی انجام داد.

امنیت سایبری جنبه‌ی مهمی در حفاظت از اطلاعات حساس و ایمن‌سازی زیرساخت‌های حیاتی برای مقابله با تهدیدات سایبری مدرن است. با افزایش پیچیدگی و فراوانی حوادث امنیتی، تقاضای فزاینده‌ای برای توسعه راه‌حل‌های نوآورانه فراتر از توانایی‌های انسانی فعلی مربوط به اقدامات امنیت سایبری وجود دارد. هوش مصنوعی را می‌توان در حوزه‌های بی‌شماری از امنیت سایبری مورد استفاده قرار داد. این به عنوان نوآوری فناورانه برای افزایش حفاظت سایبری با تسهیل تشخیص سریع‌تر و در زمان واقعی تهدید برای تهدیدات شناخته شده و ناشناخته، خودکار کردن فرآیندها برای به حداقل رساندن خطای انسانی و تصمیم‌گیری بهینه ظاهر شد. استفاده از قدرت هوش مصنوعی در امنیت سایبری، قابلیت‌های دفاعی فوق‌العاده‌ای را در برابر تهدیدات سایبری دائمی در حال تغییر آینده ایجاد می‌کند و در عین حال پرسنل امنیت سایبری را با اطلاعات تهدید و آینده‌نگری فعال برای محافظت از دارایی‌های حیاتی و اطلاعات محرمانه با دقت و اثربخشی بی‌نظیر توانمند می‌سازد. از طریق بررسی مطالعات انجام شده، کاربردهای گسترده هوش مصنوعی در امنیت سایبری مانند تشخیص نفوذ، شبیه‌سازی پیش‌بینی‌کننده و مدیریت خودکار پاسخ اضطراری مورد تجزیه و تحلیل قرار گرفته‌اند. پتانسیل آینده هوش مصنوعی در امنیت سایبری جهشی رو به جلو در گسترش مکانیسم‌های حفاظتی برای ارزیابی نقاط قوت و ضعف بردارهای حمله برای جلوگیری از حمله خصمانه خواهد داشت (تمارا، ۲۰۲۴).

اکثر روش‌هایی که می‌توان بوسیله‌ی هوش مصنوعی انجام داد، به حل مسائلی در زمینه‌ی امنیت سایبری از جمله پردازش زبان طبیعی، یادگیری ماشینی، زبان‌شناسی محاسباتی و تجزیه و تحلیلی مرتبط هستند که ماهیت برون‌یابی و آموزنده دارند. معمولاً، راه‌حل‌های هوش مصنوعی، پایگاه دانش خود را از طریق داده‌های ارائه شده توسط متخصصان یا داده‌های حاصل از تراکنش‌های اجرا شده در سیستم‌های موجود ایجاد می‌کنند. هنگامی که داده‌های مازاد به سیستم‌های هوش مصنوعی ارائه می‌شود، به پاسخ‌های تدریجی دقیق‌تری منجر می‌شود که در نهایت از کارشناسان و متخصصان انسانی پیشی می‌گیرند. در امنیت سایبری، هوش مصنوعی از تکنیک‌های یادگیری ماشینی ساخته شده تا با طبقه‌بندی اطلاعات ورودی به عنوان اطلاعات قابل‌اعتماد یا غیرقابل‌اعتماد، خطرات را شناسایی کرده و آنها را کاهش دهد. هوش مصنوعی را می‌توان به چند روش مختلف آموزش داد، از جمله یادگیری تحت نظارت که زمانی است که مدیر فعالیت‌های یادگیری سیستم را کنترل می‌کند؛ یادگیری بدون نظارتی که زمانی است که الگوها توسط سیستم شناسایی می‌شوند؛ و یادگیری تقویتی که از آزمون و خطا برای حل مسائل بدون تغذیه‌ی داده‌های سیستم استفاده می‌کنند.

نقش هوش مصنوعی در امنیت سایبری

امنیت سایبری، طیف گسترده‌ای از موضوعات را در امنیت اطلاعات از رایانه‌های شخصی گرفته تا بازیابی بلایا جهت آموزش آگاهی امنیتی دربرمی‌گیرد که ارتباط قوی با هوش مصنوعی دارد. پرسنل امنیت سایبری در عصر کنونی با چالش‌های

متعددی از جمله کمبود منابع، افزایش پیچیدگی عاملان تهدید از جمله دولت‌ها، تخصص ناکافی، حرکت نامحدود اطلاعات مبادلاتی و زمان ناکافی برای انجام وظایف محوله مواجه هستند. حوادث امنیت سایبری با سرعت قابل توجهی در حال رشد هستند، از جمله اثرات منفی که نیاز به بهبود کنترل‌های امنیتی را افزایش داده است. حوزه‌های مختلفی از امنیت سایبری وجود دارد که هوش مصنوعی می‌تواند به منظور مقابله با چالش‌های فوق‌الذکر آنها را ارائه دهد، از جمله فرمول‌بندی پاسخ‌های از پیش برنامه‌ریزی‌شده، تسریع در تحلیل ناهنجاری‌های رفتاری، و افزایش دقت تشخیص تهدید، سازمان‌دهی عملیات پاسخ به تهدید. کنترل‌های امنیت سایبری در یک سازمان را می‌توان با یکپارچه‌سازی هوش مصنوعی از جمله جلوگیری از هرزنامه، کشف آسیب‌پذیری و طبقه‌بندی اطلاعات به عنوان مخرب یا خوش‌خیم، بهبود بخشید. برخی از فعالیت‌های امنیت سایبری که می‌توان با استفاده از هوش مصنوعی افزایش داد عبارتند از: پیشگیری از نفوذ، نظارت بر مرکز عملیات امنیت، اصلاح سریع آسیب‌پذیری، و نظارت بر دارک وب (وب تاریک).

هوش مصنوعی به دلیل توانایی آن در ارزیابی تهدیدات امنیتی در زمان واقعی و انجام اقدامات مناسب، به عنوان یک جزء کلیدی امنیت سایبری ظاهر شده است. هوش مصنوعی اکنون تاثیر بیشتری در شناسایی و توقف حملاتی دارد که کسب‌وکارها را در لبه‌ی پیشرفت نگه می‌دارد. شناسایی و پیشگیری از تهدید محور اصلی نقش هوش مصنوعی در امنیت سایبری است. اگر تهاجم‌ها و حملات سایبری با استفاده از الگوریتم‌های هوش مصنوعی صورت گیرد، دفاع در برابر آنها نیازمند تکنولوژی‌های پیشرفته‌تری است و استفاده از آن برای جمع‌آوری و تحلیل داده‌ها ممکن است به نقض حریم خصوصی کاربران منجر شود. همچنین ممکن است در برخی موارد نتواند به درستی پیش‌بینی کند که چگونه یک حمله سایبری انجام خواهد شد، که این مسئله می‌تواند به کاهش امنیت سایبری منجر شود. تحقیقات بر روی ارتقاء توانایی‌های هوش مصنوعی برای تشخیص و پیشگیری از حملات سایبری، شناسایی الگوها و رفتارهای مشکوک و اجرای تدابیر امنیتی موثر می‌تواند بهبودات قابل توجهی در امنیت سایبری ایجاد کند. همچنین بررسی تجزیه وتحلیل داده‌ها به منظور شناسایی الگوها و رفتارهای غیرعادی کاربران، می‌تواند به تشخیص زودرس حملات سایبری و پیشگیری از آنها کمک کند و ترویج استفاده از فناوری‌های رمزنگاری پیشرفته برای حفاظت از داده‌ها و جلوگیری از دسترسی غیرمجاز به آنها، می‌تواند بهبود قابل توجهی در امنیت سایبری ایجاد کند. از یافته‌های اصلی از تحقیقات در زمینه‌ی تاثیر هوش مصنوعی بر افزایش امنیت سایبری و حفاظت از داده‌ها این است که استفاده از هوش مصنوعی می‌تواند بهبود چشمگیری در تشخیص، پیشگیری و مدیریت حملات سایبری فراهم کند و از طریق تحلیل داده‌های بزرگ، شناسایی الگوهای مشکوک، اجرای تدابیر امنیتی خودکار و بهبود سیستم‌های تشخیص نفوذ، می‌تواند بهبود قابل توجهی در امنیت سایبری ایجاد کند و به کاهش خطرات امنیتی در فضای آنلاین کمک کند (محمودی و بحرکاظمی، ۱۴۰۳).

هوش مصنوعی که با سرعت بسیار زیاد در زندگی روزمره ادغام می‌شود، پتانسیل بالایی جهت شکل‌دهی به چشم‌انداز دیجیتالی را بهمراه دارد. موضوع امنیت سایبری از آنجایی که می‌تواند بر همه چیز، از امنیت داده‌های شخصی گرفته تا استراتژی‌های دفاع ملی، تأثیر بگذارد، به طور فزاینده‌ای ضروری و حیاتی می‌باشد. ارتباط بین هوش مصنوعی و امنیت سایبری سه بُعد دارد: (۱) امنیت سایبری هوش مصنوعی که استانداردسازی هوش مصنوعی را پوشش می‌دهد؛ (۲) استفاده از هوش مصنوعی برای حمایت از امنیت سایبری که مدافعان امنیت سایبری را توانمند می‌نماید؛ (۳) استفاده از هوش مصنوعی برای اهداف مخرب که پتانسیل هوش مصنوعی را برای ایجاد تهدیدات جدید بررسی می‌نماید. در حالیکه جنبه‌های امنیت سایبری

هوش مصنوعی مورد توجه زیادی قرار گرفته، شواهد نشان می‌دهد که استفاده از هوش مصنوعی برای امنیت سایبری و علیه امنیت سایبری به سرعت در حال توسعه است (پولونا و تریستان[1]، ۲۰۲۴).

مزایای هوش مصنوعی در امنیت سایبری

هوش مصنوعی مزایایی برای امنیت سایبری دارد. پاسخ حادثه را می‌توان با هوش مصنوعی تغییر داد تا با زمان پاسخگویی با سرعت بالاتر، کارآمدتر باشد. مثبت کاذب می‌تواند سربار اضافی برای تیم‌های عملیات امنیتی ایجاد کند زیرا هر تهدید بالقوه باید مورد تحقیق قرار گیرد. هوش مصنوعی می‌تواند بار روی تیم‌های مرکز عملیات امنیت را با کاهش تعداد موارد مثبت کاذب تولید شده با سیستم‌های تشخیص تهدید معاصر ایجاد نمود. در روش مشابه، یادگیری ماشینی ناشی از هوش مصنوعی نتایج را با اعتبار بیشتری نسبت به سیستم‌های تشخیص تهدید معاصر تسهیل می‌کند. هوش مصنوعی می‌تواند نمای کلی یک حادثه را ارائه دهد. هوش مصنوعی همچنین از قابلیت اطمینان کمتری در پیکربندی مستقیم انسانی برخوردار است زیرا می‌تواند امضاهای امنیتی خود را ایجاد کند که در پیشگیری از تهدیدات امنیتی جدید موفق‌تر هستند. سیستم‌های امنیتی که با هوش مصنوعی فعال می‌شوند، می‌توانند زمان لازم را در اختیار تحلیل‌گران قرار دهند تا بر سایر تلاش‌هایی که هوش مصنوعی قادر به انجام آن‌ها نیست، کار کنند. تشخیص حملات ناشناخته، صلاحیت کلیدی هوش مصنوعی است. هوش مصنوعی این توانایی را دارد که با یادگیری از رویدادهای قبلی به خطرات جدید تبدیل شود، به این معنی که کنترل‌های امنیتی می‌توانند برای تبدیل شدن به اضافه کاری هوشمندتر و موفقیت‌آمیزتر و کاهش احتمال پیشروی مسائل امنیتی پیشرفت کنند. بسیاری از موقعیت‌های مکرر و پرزحمت امنیت سایبری را می‌توان با هوش مصنوعی که شامل مدیریت حادثه و تشخیص تهدید می‌شود، خودکار کرد. عملیات امنیت سایبری را می‌توان به منظور همگامی با افزایش تقاضا برای دفاع امنیتی تغییر داد. الگوریتم‌های هوش مصنوعی به طور پیشگیرانه مسائل و خطرات امنیتی را قبل از بهره‌برداری به سازمان‌ها کمک می‌کنند تا از رویدادهای امنیتی قبل از ظهور آنها جلوگیری کنند. هوش مصنوعی همچنین می‌تواند به شخصی‌سازی زمان واقعی فیلترینگ وب کمک کند تا کنترل امنیتی برای افراد به منظور محافظت از آنها در برابر محتوای مخرب و ویژگی‌های وب را فراهم آورد. هوش مصنوعی را می‌توان با خطوط لوله‌ی DevOps ادغام کرد تا کد هوشمندتر و ایمن‌تر ایجاد کند.

تکامل امنیت سایبری با هوش مصنوعی

امنیت، یکی از ضروری‌ترین نیازهای جامعه است که انواع مختلف امنیت فردی، دارایی، اطلاعات و اسناد را پوشش می‌دهد. گستردگی دسترسی به اینترنت در سطوح مختلف جامعه و پیدایش روزافزون برنامه‌های کاربردی جهت تبادل اطلاعات، مخاطرات دنیای سایبری را به یک مسئله مهم تبدیل کرده است. حضور هوش مصنوعی توانسته امنیت سایبری را نیز به یک امنیت هوشمند تبدیل نماید. به بیانی دیگر، هوش مصنوعی با شناسایی تهدیدات، خنثی‌سازی آنها و یا پیش‌بینی حملات محتمل‌الوقوع، تاثیر بسزایی در تامین امنیت گذاشته است. اخیراً تلاش‌هایی برای استفاده از تکنیک‌های هوش مصنوعی را طیف وسیعی از کاربردهای امنیت سایبری صورت گرفته است. انعطاف‌پذیری بیشتر بوسیله‌ی سیستم‌های هوش مصنوعی برای سازگاری با سناریوهای در حال تحول در چشم‌اندازی تهدیدآمیز ارائه می‌شود که دائماً در حال تغییر هستند. برخی از توابع برای مقابله با حملات سایبری از هوش مصنوعی در دسترس هستند. یک تابع، پیش‌بینی ناهنجاری است که داده‌ها را به منظور پیش‌بینی شناسایی مسائل امنیتی و کمک به تقویت کنترل‌های دفاعی برای محافظت در برابر حملات خاص، بررسی

[1]- Polona & Tristan

می‌کند. ابزار دیگری که هوش مصنوعی ارائه می‌کند، کشف ناهنجاری نام دارد که می‌تواند ناهنجاری‌ها را با برنامه‌های کاربردی، ویژگی‌های وب و زیرساخت شبکه با توانایی بیشتر برای ایجاد هشدار جهت تحقیقات بیشتر و اقدامات پیشگیرانه شناسایی نماید. آخرین ابزار هوش مصنوعی در برابر حملات سایبری به عنوان پاسخ حمله نامیده می‌شود که حملات را فوراً بدون دخالت انسان مسدود می‌کند.

تکامل هوش مصنوعی در امنیت سایبری

فناوری در حال توسعه، امکان رشد سریع در تکامل هوش مصنوعی را در قرن بیست و یکم را فراهم می‌کند. با اینحال، دهه-های مختلف تحقیق، به رشد و توسعه‌ی سریع هوش مصنوعی کمک کرده است. تحقیقات توسط آلن تورین (۲۰۰۹) در اواسط قرن بیستم با معرفی آزمون تورینگ برای ارزیابی هوش در ماشین‌ها و سپس توسط جان مک‌کارتی (۱۹۸۷) برای معرفی مفهوم عمومیت در هوش مصنوعی انجام شده است. اگرچه در اواخر قرن بود که نظریه‌های مفهومی به پیاده‌سازی و اجراهای محسوس تبدیل شدند، اما این پیشرفت‌ها همچنان ادامه داشت. در طول دهه‌ی ۱۹۹۰، دنیای فناوری با افزایش قدرت محاسباتی و توسعه‌ی امیدوارکننده در سیستم‌های تولید و پردازش داده مواجه شد. مفهوم یادگیری ماشینی در هر زمینه‌ی دیگری از برنامه‌ها رواج یافت و به منصه‌ی ظهور رسید. رشد و توسعه‌ی اینترنت با افزایش تصاعدی در قابلیت محاسباتی در فناوری پردازش، پتانسیل واقعی معماری شبکه عصبی را با قابلیت تحلیل پیچیده‌ی آن نشان داد. در همان زمان در اواخر دهه‌ی ۱۹۰۰، ارتش ایالات متحده بر نیاز به هوش مصنوعی برای ایمن‌سازی زیرساخت اطلاعات ملی تأکید نمود. هوش مصنوعی برای تشخیص نفوذ شبکه و مدیریت تأثیرات حمله‌ی سایبری توصیه می‌شود، زیرا می‌تواند به تجزیه‌وتحلیل حجم وسیعی از داده‌ها برای شناسایی الگوهای حمله و امضاهای حمله، اطلاع‌رسانی به ابزارهای نفوذ شبکه و بهبود قابلیت‌های تصمیم‌گیری کمک کند. در آن مرحله‌ی اولیه‌ی هوش مصنوعی، برنامه‌ریزی توسط مرکز ملی حفاظت از زیرساخت (NIPC) انجام شد تا نرم‌افزار مبتنی بر هوش مصنوعی توسعه یافته توسط آزمایشگاه‌های ملی Sandia (SNL) را در سیستم نظارت بر پیمان کنترل تسلیحات (ACTMS) ادغام کند، جایی که سیستم تعبیه شده‌ی توسعه یافته با سنسورهای عامل هوشمند جهت تشخیص حملات در زیرساخت‌های حیاتی و مهم مدلسازی شده است.

گرفتن و درک ابهامات جهت تجزیه‌وتحلیل امنیت برای امنیت سایبری لازم و ضروری است. از آنجایی که مدل‌های گراف سنتی در پشتیبانی از مکانیسم‌های دفاعی شبکه دارای محدودیت‌هایی هستند، زیرا محدودیت‌هایی برای رسیدگی به آسیب‌پذیری‌های ناشناخته در زمان واقعی دارند، شبکه‌ی Bayesian برای غلبه بر این چالش‌ها مورد استفاده قرار گرفت. نمایش گرافیکی رابطه‌ی علت و معلولی بین رویدادها در شبکه‌ی Bayesian برای ابهامات از جمله الگوهای حمله‌ی بی‌سابقه، توالی ناقص سوءاستفاده‌ها و محدودیت‌های حسگرهای تشخیص ناهنجاری موثر نشان داده شد. نویسندگان نشان دادند که این مدل می‌تواند به روابط علّی در حملات سایبری و جداول احتمال شرطی (CPTs) برای ثبت احتمال سناریوهای حمله‌ی شناخته شده و ناشناخته منجر شود. هوش مصنوعی از دهه‌ی ۲۰۱۰ با اختصاص رویکردهای پیشگیرانه‌تر نسبت به اقدامات واکنشی انجام شده در دهه‌های قبل، به یک مکانیسم پیشگیری کامل و مشخص پیشرفت نمود. تکنیک‌های مدرن که در ابتدا به شیوه‌های مبتنی بر قانون در امنیت سایبری با هوش مصنوعی وابسته بودند، از مدل‌های یادگیری ماشینی سنتی به استراتژی‌های یادگیری هوش مصنوعی پویاتر و سازگارتر برای ارائه راه‌حل‌های امنیت سایبری تغییر کردند. در همین حال، سیستم‌های هوش مصنوعی مدرن می‌توانند با حجم وسیعی از داده‌ها در زمان واقعی تحلیل و کار کنند تا پوشش امنیتی جامع‌تری را در مقایسه با کمبود مقیاس و پیچیدگی در مدل‌های قبلی ارائه دهند. با اینحال همانطوری که فناوری‌های هوش مصنوعی بسیار فعال‌تر و کارآمدتر می‌شوند، هوش مصنوعی متخاصم شروع به فرار از شناسایی یا ایجاد حملات پیچیده می-نماید.

هوش مصنوعی در خدمات مالی: امنیت سایبری و حفاظت از تقلب

سیستم‌های هوش مصنوعی و کاهش خطرات امنیت سایبری و کلاهبرداری

بسیاری از موسسات مالی گزارش دادند که در حال حاضر از سیستم‌های هوش مصنوعی در عملیات‌های مختلف استفاده می‌کنند، و برخی در حال ارزیابی یا آزمایشی ابزارهای مبتنی بر هوش مصنوعی برای حمایت از کارایی کارمندان در تحقیقات و وظایف گزارش‌نویسی هستند. در حالیکه اکثر موسسات مالی گزارش کرده‌اند که سال‌ها از سیستم‌های هوش مصنوعی استفاده کرده‌اند، تکامل در کاربرد و استقرار سیستم‌های هوش مصنوعی بسته به موسسه متفاوت است و همچنان در حال تکامل می‌باشد. خصوصاً، ابزارهای هوش مصنوعی برای کشف تقلب، با طیف گسترده‌ای از موسسات مالی به عنوان بخشی از استراتژی‌های مدیریت ریسک بیش از یک دهه استفاده شده است. برخی از موسسات مالی گزارش دادند که چندین سال پیش استفاده از هوش مصنوعی را برای امنیت سایبری آغاز نمودند. انواع مختلفی از ابزارهای امنیت سایبری که موسسات مالی معمولاً برای کاهش خطرات امنیت سایبری استفاده می‌کنند، اکنون هوش مصنوعی را در خود جای داده و گزارش‌ها، مؤسسات را چابک‌تر از گذشته می‌کنند. مؤسسات مالی نمونه‌هایی از ترکیب روش‌های هوش مصنوعی پیشرفته تشخیص ناهنجاری و تجزیه و تحلیل رفتار را در حفاظت از نقطه پایانی موجود، تشخیص/پیشگیری از نفوذ، پیشگیری از اتلاف داده‌ها و ابزارهای دیوار آتش ارائه کردند. ابزارهای مبتنی بر هوش مصنوعی جایگزین رویکرد امنیت سایبری تشخیص تهدید مبتنی بر امضا در بسیاری از موسسات مالی هستند. ابزارهای هوش مصنوعی می‌توانند به شناسایی فعالیت‌های مخربی کمک کنند که بدون امضای مشخص و شناخته شده ظاهر می‌شوند. این قابلیت در مواجهه با تهدیدات سایبری پیچیده‌تر و پویایی لازم و حیاتی است که ممکن است از ابزارهای مدیریت قانونی سیستم برای مثال برای جلوگیری از شناسایی امضا استفاده نمایند.

طبق بررسی‌های انجام شده، پذیرش فزاینده‌ی هوش مصنوعی، از جمله هوش مصنوعی مولد، این پتانسیل را دارد که به طور قابل‌توجهی کیفیت و کارایی هزینه‌ی عملکردهای مدیریت امنیت سایبری و ضدتقلب را بهبود بخشد. بسیاری از شرکت‌ها به اتوماسیون برای امور وقت‌گیر و کار فشرده‌ی ضدکلاهبرداری و امنیت سایبری متکی هستند. هوش مصنوعی و هوش مصنوعی مولد می‌توانند این فرآیندها را با جمع‌آوری و پردازش مجموعه‌های داده‌ی گسترده‌تر و عمیق‌تر و استفاده از تحلیل‌های پیچیده‌تر تقویت نمایند. این فناوری‌ها همچنین می‌توانند به مؤسسات کمک کنند تا از امنیت سایبری فعال‌تر و موقعیت‌های پیشگیری از کلاهبرداری استفاده کنند. به‌عنوان مثال، هوش مصنوعی مولد می‌تواند برای ارائه‌ی فرصت‌هایی برای آموزش کارکنان و مشتریان در مورد اقدامات امنیتی سایبری و کشف و پیشگیری از تقلب یا برای تجزیه و تحلیل اسناد سیاست داخلی و ارتباطات برای شناسایی و اولویت‌بندی شکاف‌ها در این اقدامات استفاده گردد (گزارش وزارت خزانه‌داری ایالات متحده‌ی آمریکا[1]، ۲۰۲۴).

هوش مصنوعی در زمینه‌ی حفاظت از داده‌ها

مقررات پارلمان اروپا و شورای مقررات عمومی حفاظت از داده‌ها (۲۰۱۶) به معنای هر گونه اطلاعات مربوط به یک شخص حقیقی شناسایی شده یا قابل شناسایی است. علاوه بر این، مقررات حفاظت از داده‌های عمومی صراحتاً مدت نمایه‌سازی را در ماده‌ی ۴ مشخص می‌کند. به نظر می‌رسد فناوری قادر به استنباط ویژگی‌های شخصی خاص بر اساس داده‌هایی است که به طور آنی به آن مربوط نمی‌شود. به همین دلیل بسیار مهم است که داده‌های مورد استفاده به عنوان مبنای الگوریتم یادگیری مناسب باشد تا از تحریف، سوگیری و تبعیض جلوگیری شود. با وجود این واقعیت که پردازش دسته‌های خاصی از داده‌های شخصی بر اساس ماده‌ی ۹ مقرارت حفاظت از داده‌های عمومی ممنوع است، الگوریتم‌ها می‌توانند این اطلاعات را از طریق

[1]- U.S. Department of the Treasury

داده‌های دیگر با رعایت مرزهای حریم خصوصی استخراج کنند. حفاظت از داده‌ها، مزایای مرتبط با داده‌های بزرگ را محدود نمی‌کند، بلکه داده‌های بزرگ می‌تواند در کنار حفاظت از حریم خصوصی، مزایای خود را عرضه کند. شفافیت همچنان یک اصل مهم حفاظت از داده است و می‌تواند با روش‌های نوین اعمال شود. پاسخگویی نیز در داده‌های بزرگ بسیار مهم است. در مجموع، حفاظت از داده‌های شخصی در بستر داده‌های بزرگ چالش‌برانگیز است اما با بهره‌گیری از ابزارهای مناسب، امکان‌پذیر و ضروری است. طبق ماده‌ی ۲۲ مقررات حفاظت از داده‌های عمومی، موضوع داده‌ها این حق را خواهد داشت که تنها براساس پردازش خودکار از جمله نمایه‌سازی، تحت تصمیم‌گیری قرار نگیرد. بنابراین افراد ممکن است به هر نوع پردازش داده‌های خود که بدون نظارت یا دخالت انسانی انجام می‌شود، اعتراض کنند. مطابق با مواد ۱۵-۱۳ مقررات حفاظت از داده‌های عمومی مربوط به اطلاعات و دسترسی به داده‌های شخصی، کلیه‌ی سازمان‌هایی که قصد دارند داده‌ها را در الگوریتمی قرار دهند که پس از آن تصمیمی در مورد یک فرد اتخاذ می‌کند، موظف هستند به فرد اطلاع دهند که در چنین مواردی پردازش صورت خواهد گرفت. براساس مفاد مقررات حفاظت از داده‌های عمومی، تصمیم‌گیری فردی خودکار تحت ممنوعیت کامل نیست، برخی از استثنائات در ماده‌ی ۲۲ (بند ۲) تعیین شده است: «این نوع تصمیم‌گیری برای انعقاد یا اجرای قرارداد بین طرفین ضروری است. موضوع داده و یک کنترل‌کننده‌ی داده توسط قانون اتحادیه یا کشور عضو، مجاز است. همچنین رضایت صریح موضوع داده به تصمیم‌گیری خودکار داده شده است. داده‌کاوی می‌تواند برای ایجاد پروفایل‌های دیجیتالی مورد استفاده قرار گیرد و اجازه می‌دهد تا تصمیمات اساسی بدون اطلاع افراد گرفته شود. اگر داده‌های حاصل جنبه‌ی شخصی فرد را نادرست نشان دهند، یا داده‌ها رفتارهای فرد را بیش از حد غیرواقعی نشان دهند، چنین داده‌هایی تا حد زیادی از انتظارات شخص برای حفظ حریم خصوصی تجاوز می‌کنند. همچنین تصمیمات خودکار، ارزیابی معقول دیگران از فرد را مخدوش می‌کند (محمودی و بحرکاظمی، ۱۴۰۳).

هوش مصنوعی در حمایت از امنیت سایبری

تعداد فزاینده‌ای از شرکت‌ها مانند IBM، Google و Microsoft شروع به تبلیغات و نمایش روش‌هایی کرده‌اند که در آنها می‌توان از هوش مصنوعی برای افزایش امنیت سایبری استفاده کرد. موارد استفاده‌ی تبلیغاتی به چهار دسته تقسیم می‌شوند: تشخیص، پیش‌بینی، تجزیه‌وتحلیل و کاهش تهدید. سیستم‌های هوش مصنوعی می‌توانند تهدیدات و آسیب‌پذیری‌ها را شناسایی کنند. از نظر تهدیدات، تحقیقات نشان می‌دهد که فناوری‌های یادگیری ماشینی قادر به شناسایی بدافزار هستند. گوگل پیشنهاد می‌کند که هوش مصنوعی می‌تواند پویایی معروف به معضل مدافع را معکوس کند، به این معنی که هوش مصنوعی می‌تواند به متخصصان امنیت سایبری کمک کند تا کار خود را در تشخیص تهدید افزایش دهند. گوگل همچنین ادعا می‌کند که هوش مصنوعی مولد به «۵۱ درصد صرفه‌جویی در زمان و بازدهی با کیفیت بالاتر در خروجی تحلیل‌گر حوادث در تلاش‌های شناسایی داخلی و پاسخ آنها کمک کرده است». از نظر آسیب‌پذیریا، گوگل ادعا می‌کند که مدل هوش مصنوعی مولد آن، Gemini، کمک قابل توجهی به شناسایی آسیب‌پذیری‌های جدید کرده است (پولونا و تریستان، ۲۰۲۴).

علاوه بر تشخیص و شناسایی، سیستم‌های هوش مصنوعی قادر به پیش‌بینی تهدیدها و خطرات نیز هستند. استفاده از هوش مصنوعی را برای گزارش خطرات قطع سرویس در زمینه اینترنت اشیا (IoT) پیشنهاد می‌کند. گوگل گزارش می‌دهد که هوش مصنوعی می‌تواند بر اساس مجموعه داده‌ای از مکان‌یاب‌های مخرب منبع (URL) مرتبط با ابزار مرور ایمن پیشرفته خود پیش-بینی کند. فناوری‌های هوش مصنوعی همچنین قادر به تجزیه‌وتحلیل کد و طبقه‌بندی بدافزارها هستند. ابزار VirusTotal ابزار اسکن چندگانه‌ی بدافزار معروف متعلق به گوگل است که نشان می‌دهد چگونه هوش مصنوعی مولد می‌تواند درک یک بدافزار معین را بهبود بخشد و احتمالاً از تشخیص مثبت کاذب (یعنی فایل‌هایی که به‌طور نادرست توسط برنامه‌های آنتی ویروس به عنوان بدافزار پرچم‌گذاری شده‌اند) جلوگیری کند. بهبود در دقت جهت شناسایی و تشخیص تهدید به کارایی در پاسخگویی به تهدیدات واقعی کمک می‌کند. علاوه بر این، ENISA پیشنهاد می‌کند که الگوریتم‌های ژنتیک، نوعی از الگوریتم‌های تکاملی

هوش مصنوعی، می‌توانند برای طبقه‌بندی بدافزار استفاده شوند. در نهایت، هوش مصنوعی می‌تواند به کاهش تهدید کمک کند. راه‌حل‌های مبتنی بر هوش مصنوعی قابلیت‌های پاسخ به حادثه را اتومات نموده و در نتیجه زمان پاسخ را افزایش می‌دهند. آنها می‌توانند تهدیدها را اولویت‌بندی نموده، روندها را شناسایی کنند و در پیش‌بینی تهدیدات آینده سهیم باشند. به عنوان مثال، گوگل ادعا می‌کند که Gemini ۱۵ درصد از باگ‌های کشف شده را با موفقیت برطرف کرده است.

رویکردهای مبتنی بر هوش مصنوعی در امنیت سایبری

هوش مصنوعی ابزاری نوظهور است که راه‌حل‌های امیدوارکننده‌ای را برای مشکلات پیچیده‌ی امنیت سایبری ارائه می‌دهد. در این قسمت کاربردهای مهم و پیشرفت‌های فعلی در این زمینه‌ها بررسی گردیده و چهار زیرمجموعه‌ی کلیدی بیان می‌شود: فیشینگ، مهندسی اجتماعی، باج‌افزار و بدافزار. برای هر دسته، تکنیک‌ها و روش‌های خاصی مطرح شده که از هوش مصنوعی برای مقابله با این تهدیدات رایج بهره‌مند می‌شود. این کار از رویکرد مقایسه‌ای استفاده نموده که از تجزیه‌وتحلیل توصیفی و بحث‌های عمیق جهت روشن کردن نقاط قوت، ضعف و فرصت‌ها برای تحقیقات بیشتر در راه‌حل‌های امنیت سایبری مبتنی بر هوش مصنوعی استفاده می‌شود. دهه‌ی گذشته (۲۰۱۳-۲۰۲۳) با افزایش تهدیدات امنیت سایبری پیچیده و مخرب مالی همراه بوده است. این حوادث بزرگ، که اغلب بیش از یک میلیون دلار تأثیر مالی داشته، چالشی مهم برای امنیت جهانی و ثبات اقتصادی ایجاد می‌کنند. در نتیجه، درک تکامل و الگوهای این حملات در دهه‌ی گذشته برای محققان در این زمینه بسیار مهم بود. در مطالعه‌ای، تشدید قابل توجهی در فراوانی و پیچیدگی حملات سایبری را شناسایی کردند. حوادث DDoS در سال ۲۰۲۲ افزایش یافت، در حالیکه حملات بدافزار به طور پیوسته افزایش یافت و در سال ۲۰۲۳ به اوج خود رسید. این روند بر پیچیدگی فزاینده‌ی عاملان تهدید و آسیب‌پذیری زیرساخت‌های دیجیتال تأکید می‌کند. علاوه بر این، تأثیر ترکیبی سایر روش‌های حمله، از جمله فیشینگ و حمله‌های صفر روزه، از DDoS و بدافزار پیشی گرفته و ماهیت متنوع تهدیدات سایبری را آشکار نمود (فالوو و همکاران، ۲۰۲۴).

ارتباطات ایمن، ستون اساسی امنیت سایبری در حوزه‌ی فناوری اطلاعات می‌باشد. با اینحال، ارتباطات بی‌سیم به دلیل آسیب-پذیری ذاتی، چالشی منحصر به فرد را ارائه می‌دهد. برخلاف اتصالات سیمی، داده‌های بی‌سیم از طریق امواج رادیویی عبور نمودند و اساساً اطلاعات را پخش می‌کنند. از آنجایی که داده‌ها پخش می‌شوند، می‌توان آنها را رهگیری نمود. مهاجمان با نیت مخرب می‌توانند این ارتباط پخش را رهگیری کنند (اُکدم و اُکدم، ۲۰۲۴).

بدلیل پیشرفت در فناوری محاسبات، جامعه به سرعت در حال تغییر است. روال روزمره‌ی مردم و اشتغال، به طور قابل توجهی تحت تأثیر این امر قرار دارد. برخی از این فناوری‌ها امکان توسعه‌ی رایانه‌هایی را فراهم نموده‌اند که توانایی‌های شناختی مشابه انسان‌ها از جمله توانایی یادگیری، تصمیم‌گیری و حل مشکلات دارند. به عنوان مثال، هوش مصنوعی می‌تواند حجم عظیمی از داده‌ها را تجزیه‌وتحلیل نماید و می‌تواند در زمان استفاده از هوش قضاوت کند. زمینه‌های متعددی از تحقیقات و فناوری از کاربرد تکنیک‌های هوش مصنوعی سود می‌برند. بر کسی پوشیده نیست که اینترنت پر از داده‌های شخصی است که منجر به مشکلات امنیت سایبری زیادی می‌شود. اولاً مقدار داده، تجزیه‌وتحلیل دستی را غیرممکن می‌کند. ثانیاً ممکن است خطراتی مبتنی بر هوش مصنوعی یا افزایش تهدیدات وجود داشته باشد. علاوه بر این، هزینه‌های پیشگیری از تهدیدها به دلیل هزینه‌ی بالای استخدام متخصصان افزایش می‌یابد. توسعه و استفاده از الگوریتم‌ها برای شناسایی این خطرات نیز مستلزم صرف زمان، هزینه و تلاش زیادی است. استفاده از تکنیک‌های مبتنی بر هوش مصنوعی یک راه‌حل برای این مشکلات است. هوش مصنوعی قادر به تجزیه‌وتحلیل سریع، صحیح و کارآمد داده‌های عظیم است. یک سیستم مبتنی بر هوش مصنوعی می‌تواند حملات آینده را پیش‌بینی نماید که مشابه حملاتی هستند که قبلاً با استفاده از تاریخچه‌ی تهدید رخ داده‌اند، حتی اگر الگوهای آن حملات متفاوت باشد. هوش مصنوعی می‌تواند داده‌های گسترده‌ای را مدیریت نماید، تغییرات جدید و قابل توجهی را در حملات پیدا کند و به طور مداوم پاسخ سیستم امنیتی خود را به تهدیدات بهبود بخشد. استفاده از هوش مصنوعی در

امنیت سایبری رویکرد امنیتی سنتی را از واکنشی به پیشگیرانه و کمک به شناسایی و کاهش تهدیدات در زمان واقعی تغییر داده است.

حملات فیشینگ

اخیراً حملات فیشینگ رایج‌ترین جرایم سایبری است. آنها از ایمیل‌های جعلی استفاده می‌کنند که به نظر می‌رسد از طرف شخصی مورد اعتماد می‌باشد. این ایمیل‌ها سعی در سرقت اطلاعات ارزشمند دارند. گیرنده فریب داده می‌شود تا اطلاعات شخصی را در اختیار قرار دهد. این اطلاعات می‌تواند شامل داده‌های حساس مانند گذرواژه‌ها و جزئیات کارت اعتباری باشد. مهاجمان مانند ماهیگیران عمل می‌کنند و از یک نمای وسوسه‌انگیز برای فریب دادن قربانیان ناآگاه به دام خود استفاده می‌کنند. اطلاعات دزدیده شده می‌تواند به جرایم مالی یا اعمال مخرب دامن بزند، اما آگاهی کاربر و امنیت آنلاین قوی بهترین دفاع در برابر این تهدیدات در حال تحول است (کاپان و سورا گونال، ۲۰۲۳).

حملات فیشینگ به ایمیل محدود نمی‌شود. فیشرها از یک رویکرد پراکنده و از پیام‌های گمراه‌کننده در کانال‌های ارتباطی مختلف استفاده می‌کنند که شامل پیام‌های فوری، انجمن‌های آنلاین و رسانه‌های اجتماعی است. این پیام‌ها اغلب حاوی یک لینک فریبنده هستند که به یک وب‌سایت جعلی که برای سرقت اطلاعات شما طراحی شده، منجر می‌شود. این روش گسترده به طور قابل توجهی شانس کاربر را افزایش می‌دهد و ناآگاهانه با نام کاربری و رمز عبور خود در وب‌سایت جعلی وارد می‌شود. اینگونه است که حملات فیشینگ اعتبار ورود به سیستم را می‌دزدند. هدف مخربانه‌ی عمل فیشینگ، اغلب هوشمندانه پنهان می‌شود. بنابراین، احتیاط آنلاین بسیار مهم است. با به دست آوردن اطلاعات ورود به سیستم دزدیده شده، فیشرها پتانسیل راه‌اندازی انواع جرایم سایبری را به دست می‌آورند که همگی از یک کلیک ناآگاهانه ناشی می‌شوند. یادگیری ماشینی و یادگیری عمیق می‌توانند ابزارهای قدرتمندی در شناسایی الگوهایی باشند که اهداف مخرب را در این حملات آشکار می‌کنند. این تکنیک‌ها مقادیر زیادی از داده‌ها را برای تشخیص تلاش‌های فیشینگ در زمان واقعی تجزیه و تحلیل می‌کنند. شبیه به هوش خودکار، یادگیری ماشینی و یادگیری عمیق به عنوان ابزار تصمیم‌گیری قدرتمند در سیستم‌های اطلاعات مدیریت عمل می‌کنند. حملات فیشینگ یک تهدید دائمی در امنیت سایبری است. عمر کوتاه کمپین‌های فیشینگ می‌تواند شناسایی مهاجمان را دشوار کند. با اینحال، استراتژی‌های کاهش موثر همچنان می‌توانند اجرا شوند، که عبارتند از:

همکاری اجرایی: بهبود اشتراک‌گذاری اطلاعات و همکاری برای مبارزه با حملات فیشینگ بسیار مهم است. همکاری دیجیتالی قوی‌تر مفید است و به طور بالقوه از حملات آینده جلوگیری می‌کند. بنابراین، می‌توان تهدیدات را با سرعت بیشتری از بین برد.

آموزش کاربر: اگرچه حذف کامل فیشینگ گریزان است، آموزش کاربر در تشخیص نشانه‌های بصری مانند URLهای مشکوک و تناقضات وب‌سایت می‌تواند آسیب‌پذیری را به طور قابل توجهی کاهش دهد، به ویژه برای کاربران تازه‌کار.

نیاز به آموزش مستمر: چندین مطالعه نشان داده است که بسیاری از کاربران تازه‌کار اینترنت، اغلب به آن توجه نمی‌کنند. این بی‌توجهی می‌تواند آنها را بیشتر مستعد حملات فیشینگ کند. این امر مستلزم ابتکارات آموزشی مداوم و تکراری برای آگاه نگهداشتن کاربران در مورد تاکتیک‌های فیشینگ و روش‌های فریب مورد استفاده مهاجمان است.

انجمن‌های فیشینگ آنلاین: جوامع آگاه از فیشینگ آنلاین به عنوان منابع ارزشمند برای کاربران، اغلب داده‌هایی را در مورد تلاش‌های فیشینگ، از جمله آدرس‌های اینترنتی در لیست سیاه، جمع‌آوری می‌کنند. اینها ابزار مفیدی هستند، اما برای محافظت قوی، کاربران باید از شاخص‌های امنیتی وب گسترده‌تر نیز آگاه باشند.

امنیت سایبری در مهندسی اجتماعی

پیشرفت‌های اخیر در رسانه‌های اجتماعی، وظایف را خودکار نموده و سهولت و راحتی را بیشتر نموده، اما افزایش نگرانی‌های امنیتی را نیز بدنبال دارد. سرقت هویت، کلاهبرداری مالی و دسترسی غیرمجاز برخی از مهم‌ترین تهدیدها هستند. استفاده از نرم‌افزار قابل اعتماد و ایمن برای مصون ماندن بسیار مهم است. تحقیق در مورد امنیت سایبری کمک می‌کند تا این خطرات را درک کرده و راه‌هایی برای محافظت ایجاد نمود. عصر دیجیتال، حضور آنلاین افراد را گسترش می‌دهد زیرا افراد قسمت اعظم زندگی‌شان را به صورت آنلاین به اشتراک می‌گذارند. حملات مهندسی اجتماعی، که به جای آسیب‌پذیری‌های فنی، از اعتماد انسانی سوء استفاده می‌کنند، به طور فزاینده‌ای رایج می‌شوند. در این حملات، عوامل مخرب افراد را دستکاری می‌کنند تا به داده‌های حساس دسترسی پیدا کنند. حتی اگر پیشرفت‌های امنیت سایبری می‌تواند تأثیر چنین حملاتی را به حداقل برساند، تحقیقات نشان می‌دهد که عنصر انسانی یک عامل حیاتی در ایمنی آنلاین باقی می‌ماند (سالاما و تورجمن، ۲۰۲۳).

حملات مهندسی اجتماعی، که از دستکاری روانی برای دستیابی به اهداف مخرب سوءاستفاده می‌کنند، به دلیل در دسترس بودن گسترده‌ی فناوری و گسترش ارتباطات آنلاین در حال افزایش هستند. با اینحال، تحقیقات در زمینه‌ی مهندسی اجتماعی در حوزه‌ی امنیت سایبری محدود است. این محدودیت را می‌توان به عدم وجود معیارهای یکپارچه برای ارزیابی این حملات یا کمبود استراتژی‌های کاهش موثر نسبت داد. در پژوهشی نویسندگان این شکاف مهم را با پیشنهاد یک فرآیند مبتنی بر مدل‌سازی موضوعی جدید برای مدل‌سازی حملات سایبری، برطرف می‌کنند. این فرآیند با موفقیت در مدل‌سازی حملات قلدری به کار گرفته شد، جایی که مهاجمان به وضوح از تکنیک‌های دستکاری روانی استفاده کردند. این مدل به دقت بالایی در تشخیص هدف ارتباطی مهاجمان دست یافت. استانداردسازی دانش و فرآیندها می‌تواند راه را برای توسعه‌ی راه‌حل‌های قوی‌تر و جامع‌تر در برابر این تهدیدات آنلاین همیشه در حال تکامل هموار کند. اثربخشی فرآیند مدل‌سازی بر پتانسیل آن برای استفاده در آینده در برابر طیف وسیع‌تری از حملات مهندسی اجتماعی پیش‌بینی نشده تاکید می‌کند. تحقیقات اخیر امنیت سایبری، اغلب فاقد راه‌حل‌های جامع برای حملات مهندسی اجتماعی هستند. تحقیقات مؤثر باید دیدگاه‌های متنوعی را در مورد روش‌های حمله دربرگیرد. با اینحال، به دست آوردن درک کامل از موضوع همچنان دشوار است. مهاجمان به طور مداوم تاکتیک‌های خود را تطبیق می‌دهند و به دفاعی نیاز دارند که این تهدیدات در حال تغییر را پیش‌بینی و مقابله کند. این تهدید مداوم بر نیاز به تحقیق و توسعه‌ی دائمی در امنیت سایبری تاکید می‌کند.

باج‌افزار: تهدیدی روبه‌رشد در چشم انداز امنیت سایبری

باج‌افزار نوعی نرم‌افزار مخرب است که فایل‌های کاربر را رمزگذاری نموده و آنها را غیرقابل‌دسترسی می‌کند. هدف آن اخاذی از قربانی در ازای باز کردن قفل پرونده‌ها است. یک حمله‌ی باج‌افزار بزرگ به نام WannaCry در سال ۲۰۱۷ جهان را تحت تأثیر قرار داد. این رویداد به طور قابل توجهی آگاهی عمومی را از تهدیدات امنیت سایبری افزایش داد. در سال‌های اخیر، تکثیر باج‌افزارها به یک نگرانی بزرگ تبدیل شده و خسارات مالی قابل‌توجهی، آسیب‌های اعتباری، و اختلالات عملیاتی را به افراد و سازمان‌ها وارد کرده است. باج‌افزار در سال ۱۹۸۹ ظهور کرد و به سرعت به یک تهدید پیچیده و گسترده تبدیل شد. تکنیک‌های رمزگذاری آن به‌طور فزاینده‌ای پیچیده‌تر شدند، توانایی آن برای گسترش و فرار از شناسایی افزایش یافته ، و ظرفیت آن برای اخاذی از قربانیان تشدید شده است. خسارات جهانی ناشی از حملات باج‌افزار در مسیری قرار دارد که در سال‌های آتی از صدها میلیارد دلار فراتر رفته و حملات جدید در عرض چند ثانیه اتفاق می‌افتد. خسارت تجمعی در سراسر جهان ناشی از حوادث باج‌افزار به طور پیوسته در طول زمان در حال افزایش است (رازاولا و همکاران، ۲۰۲۳).

در حالیکه تحلیلگران انسانی برای همگام شدن با حجم روزافزون داده‌ها تلاش می‌کنند، هوش مصنوعی در این حوزه برتری دارد. توانایی آن در تجزیه‌وتحلیل مجموعه داده‌های عظیم باعث می‌شود که آنها برای تشخیص باج‌افزار بسیار موثر باشند. در

این زمینه، الگوریتم‌های هوش مصنوعی بر روی مجموعه‌ای عظیم از نرم‌افزارهای بدخیم و مخرب آموزش داده می‌شوند. با تجزیه‌وتحلیل رفتار این برنامه‌ها، الگوریتم‌ها یاد می‌گیرند که ویژگی‌های مشخصه‌ای را شناسایی کنند که باج‌افزار را از برنامه-های کاربردی قانونی متمایز می‌کند. این دانش به دست آمده آنها را قادر می‌سازد تا حتی انواع باج‌افزارهای جدید را شناسایی کنند، حتی آنهایی که قبلاً هرگز با آنها مواجه نشده بودند. آگاهی کاربر نقش حیاتی در دفاع از باج‌افزار ایفا می‌کند. برنامه‌های آموزشی که به کاربران در مورد اصول باج‌افزار و سیستم‌های دفاعی فعلی آموزش می‌دهند، می‌توانند آمادگی سازمانی را به میزان قابل توجهی بهبود بخشند. همچنین به کاربران این امکان را می‌دهد که در وضعیت امنیتی کلی مشارکت داشته و خطر حملات موفقیت‌آمیز را کاهش دهند.

دفاع در برابر بدافزارها

نرم‌افزارهای مخرب که به عنوان بدافزار نیز شناخته می‌شوند، تهدیدی قابل توجه برای صنعت فناوری اطلاعات هستند. افزایش اخیر حملات بدافزار به یک چالش بزرگ تبدیل شده است. بدافزارها می‌توانند بدون مجوز به سیستم‌های کامپیوتری نفوذ کنند که منجر به پیامدهای مضر مختلفی می‌شود. این عواقب اغلب شامل سرقت اطلاعات و فساد سیستم می‌شود. محبوبیت روزافزون دستگاه‌های تلفن همراه، به ویژه دستگاه‌های دارای اندروید، ضرورت توسعه‌ی راه‌حل‌های امنیتی قوی را ایجاب می-کند. با اینحال، این پذیرش گسترده همچنین هدف بزرگتری برای آلودگی‌های بدافزار موبایل ایجاد می‌کند. برای پرداختن به این مسئله‌ی حیاتی، یک رویکرد مبتنی بر ML برای تشخیص ناهنجاری در دستگاه‌های اندروید پیشنهاد شده است سیستم آنها از قدرت سه الگوریتم یادگیری ماشینی، از جمله K-nearest همسایه (KNN)، Bayes ساده و درخت تصمیم استفاده می-کند. آنها رفتار برنامه‌های تلفن همراه را تجزیه‌وتحلیل کردند و آسیب‌پذیری‌های احتمالی بدافزار را شناسایی نمودند. روش‌های MLیک رویکرد قدرتمند برای مبارزه با تهدید روبه‌رشد بدافزار ارائه می‌دهند. این روش‌ها ابزاری را برای تجزیه‌وتحلیل و طبقه‌بندی مقادیر زیادی از داده‌ها فراهم می‌کنند. آنها به بدافزارها اجازه‌ی شناسایی می‌دهند. موفقیت‌های آنها حتی زمانی صادق است که از تکنیک‌های مبهم‌سازی برای فرار از تشخیص سنتی مبتنی بر امضا استفاده می‌کنند. یکی از رویکردهای یادگیری ماشینی توسط کومار و همکاران پیشنهاد شده است. رویکرد آنها بر اساس تکنیک طبقه‌بندی جهت دسته‌بندی فایل-های Windows PE است. این تکنیک بر روی مجموعه داده‌ی قابل توجهی از تقریباً ۱۰۰۰۰۰ نمونه بدافزار برزیلی آموزش داده شده است. هر نمونه با ۵۷ ویژگی مشخص می‌شود. نویسندگان مدل‌های مختلف یادگیری ماشین را بررسی می‌کنند و با یک مدل جنگل تصادفی به بالاترین دقت ۹۹.۷ درصدی دست می‌یابند. این نتیجه اثربخشی مدل جنگل تصادفی را در تمایز بین فایل‌های بدخیم و بدخیم نشان می‌دهد و پتانسیل آن را به عنوان یک ابزار ارزشمند برای امنیت سیستم نشان می‌دهد. ظهور مداوم انواع بدافزار جدید، که اغلب از نرم‌افزارهای قانونی تقلید می‌کنند، چالش مهمی برای شناسایی ایجاد می‌کند. علاوه بر این، توانایی بدافزار برای اصلاح پویایی ساختار داخلی خود به پیچیدگی اضافه می‌شود. برای رفع این مشکلات و بهبود کارایی تشخیص، راه‌حل‌های تحلیل پویا برای تسریع استخراج ویژگی بسیار مهم هستند. علاوه بر این، تحقیق در مورد رویکردهای تشخیص پیشرفته‌تر برای شناسایی موثر فعالیت‌های مخرب ضروری است. افزایش اخیر بدافزار «هوشمند» بر نیاز به توسعه‌ی فناوری‌های هوش مصنوعی (AI) برای شناسایی و پیشگیری از بدافزار تأکید شده است.

چالش‌ها و محدودیت‌های هوش مصنوعی در امنیت سایبری

در دنیای امروز پیشرفت و توسعه‌ی زیادی در فناوری‌های ارتباطی و اینترنت صورت گرفته و یکی از مهم‌ترین زمینه‌هایی که در آن ظاهر شده، امنیت شبکه است. از ابزارهایی مانند فایروال‌ها، نرم‌افزارهای آنتی‌ویروس و سیستم‌های تشخیص نفوذ برای اطمینان از حفاظت شبکه و تمام منابع مرتبط آن در اینترنت استفاده می کند. این رویکردها از شبکه‌ها در برابر تهدیدات

داخلی و خارجی محافظت می‌کند. هوش مصنوعی مولد نوعی فناوری هوش مصنوعی است که می‌تواند انواع مختلفی از محتوا از جمله متن، تصویر، صدا و داده‌های مصنوعی تولید کند. هیاهوی اخیر در مورد هوش مصنوعی مولد بدلیل سادگی رابط‌های کاربری جدید برای ایجاد متن، گرافیک و ویدئوهای با کیفیت بالا در عرض چند ثانیه و همچنین توانایی خلق محتواهایی است که پیش از این وجود نداشته‌اند و در واقع هوش مصنوعی مولد مبدع و مبتکر آن است. با وجود این پیشرفت‌ها و فراگیری استفاده از کاربردهای هوش مصنوعی مولد، واکنش‌های قابل توجهی نیز علیه آن وجود داشته است. زیرا علاوه بر دغدغه‌ی کشورها نسبت به عقب نماندن در توسعه این فناوری، نگرانی‌های جدی نیز در مورد به‌کارگیری و بهره‌مندی از آن در حال پررنگ شدن است که ازجمله آنها می‌توان به صحت، دقت، امنیت اطلاعات و ملاحظات اخلاقی اشاره کرد. هرچند نگرانی‌های ذکر شده فقط مرتبط با هوش مصنوعی مولد نیست و کل عرصه‌های هوش مصنوعی بطور عام را دربرمی‌گیرد، اما ویژگی ایجاد و خلق محتوای جدید بدون دخالت و کنترل انسان و ارائه تصمیمات جدید و پاسخ‌هایی که ممکن است به‌راحتی قابل ارزیابی و صحت‌سنجی نباشند به کاربران و در نتیجه تأثیرگذاری بالای این فناوری بر قدرت تفکر، انتخاب، تصمیم‌گیری و عملکردهای انسانی که بواسطه‌ی توانایی‌های هوش مصنوعی مولد ایجاد شده و به‌شدت رو به گسترش است، سطح نگرانی‌ها را افزایش داده است. این ابعاد گسترده، پیچیده و جدید از منظر فنی، اقتصادی، اجتماعی و حتی سیاسی، سیاست‌گذاران را به‌سمت تنظیم چارچوب‌ها و اصولی که به‌طورکلی براساس سطح مخاطره انواع هوش مصنوعی منجر به توسعه هدفمند و پایدار فناوری‌های این حوزه شود، سوق داده است (تقی‌زاده و خردمندنیا، ۱۴۰۳).

با وجود مزایای متعدد هوش مصنوعی، این فناوری با چالش‌هایی روبرو است که باید بدقت مدنظر قرار گیرد. شناسایی این محدودیت‌ها برای ادغام مؤثر هوش مصنوعی در چارچوب‌های امنیت سایبری اهمیت دارد:

نگرانی‌های حریم خصوصی داده‌ها

پردازش گسترده داده‌ها در سیستم‌های هوش مصنوعی مسائل حریم خصوصی قابل توجهی را به وجود می‌آورد. سازمان‌ها باید با ضرورت مضاعف استفاده از داده‌ها برای آموزش هوش مصنوعی در عین حفظ حریم خصوصی کاربران و اطمینان از انطباق با قوانینی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) مقابله کنند. دستیابی به این تعادل برای حفظ اعتماد عمومی و جلوگیری از پیامدهای قانونی حیاتی است.

سوگیری الگوریتمی

سیستم‌های هوش مصنوعی به کیفیت داده‌های استفاده‌شده برای آموزش وابسته هستند. اگر داده‌های آموزشی دارای سوگیری‌های ذاتی باشند، هوش مصنوعی ممکن است نتایج نادرستی تولید کند که به استنتاج‌های نادرست و شناسایی ناکارآمد تهدید منجر می‌شود. تحقیقات پیوسته بر اهمیت شناسایی سوگیری‌ها و راهکارهای کاهش آنها در الگوریتم‌های هوش مصنوعی تأکید دارد تا نتایج منصفانه‌ای در سناریوهای امنیت سایبری ایجاد شود.

حملات متخاصم

تکنولوژی‌های هوش مصنوعی ممکن است در برابر حملات متخاصم آسیب‌پذیر باشند که در آن موجودیت‌های مضر سعی در فریب سیستم‌های هوش مصنوعی دارند. هکرها ممکن است از نقاط ضعف در الگوریتم‌های هوش مصنوعی بهره‌برداری کنند و داده‌های ورودی را تغییر دهند تا از مهم‌ترین تدابیر امنیتی عبور کنند. بینش‌های موجود در arXiv استراتژی‌های متنوعی را که در محیط‌های متخاصم استفاده می‌شود، روشن می‌کند و جنگ تسلیحاتی ادامه‌دار بین مدافعان هوش مصنوعی و هکرها را نشان می‌دهد.

هزینه‌های بالای پیاده‌سازی

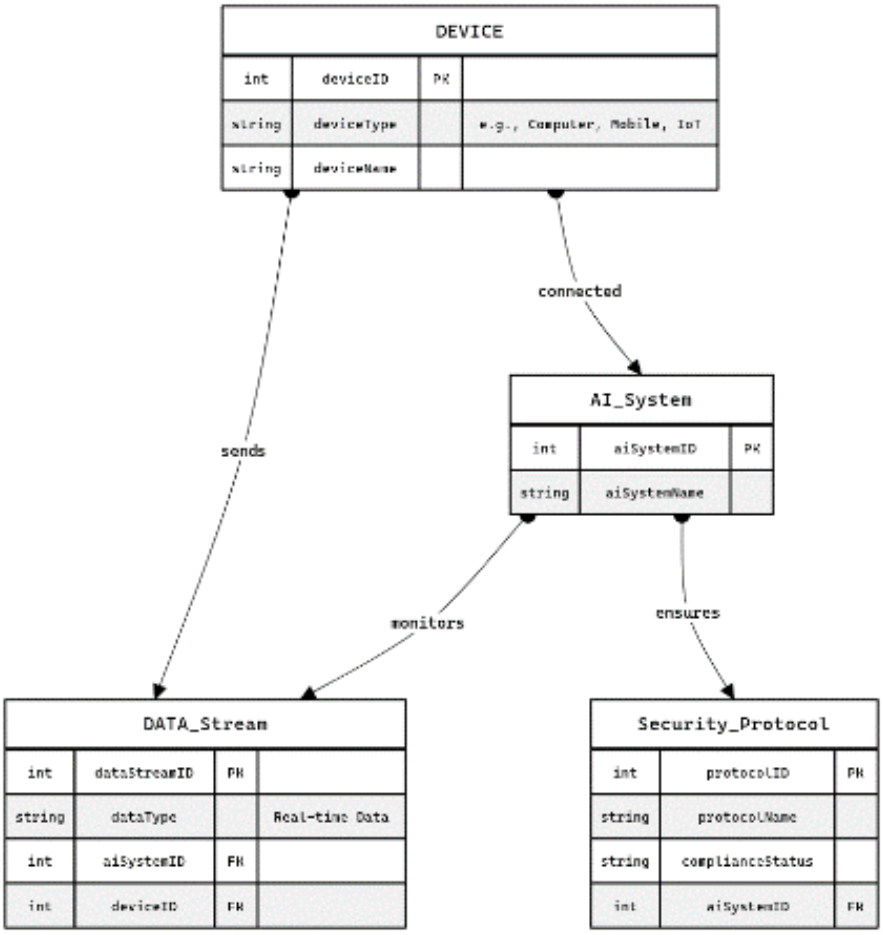
ادغام راهکارهای هوش مصنوعی در چارچوب‌های امنیتی پیشین می‌تواند هزینه‌های قابل توجهی به‌دنبال داشته باشد و به منابع گسترده‌ای نیاز داشته باشد. سازمان‌ها باید مزایای بالقوه را در مقابل سرمایه‌گذاری اولیه و تعهدات بلندمدت مرتبط با حفظ زیرساخت‌های امنیتی تقویت‌شده با هوش مصنوعی به‌دقت ارزیابی کنند.

کاربرد قدرت هوش مصنوعی برای افزایش امنیت سایبری نسل بعدی

امنیت نقطه‌ی پایانی

سیستم‌های حفاظت نقطه‌ی پایانی، رایج‌ترین نوع یادگیری ماشینی (ML) است که امروزه به کار گرفته شده است. هوش مصنوعی می‌تواند با استفاده از یادگیری ماشینی برای درک نقشه‌های رفتاری قبلی به منظور ایجاد امتیاز ریسک، در کنترل دسترسی برای نقاط پایانی موفق باشد. هوش مصنوعی همچنین می‌تواند در کنترل امنیت نقاط پایانی موبایل از طریق استفاده از یادگیری ماشینی و روش‌شناسی اعتماد صفر مؤثر باشد. مدیریت دارایی می‌تواند مسئله‌ی حیاتی برای سازمان‌ها باشد، زیرا دارایی‌های طبقه‌بندی شده بطور نادرست می‌تواند منجر به عدم گنجاندن این دارایی‌ها در محدوده‌ی کنترل‌های امنیتی حیاتی شود.

هوش مصنوعی می‌تواند مدیریت دارایی‌های فناوری اطلاعات (IT) را با بهره‌گیری از قابلیت‌های کلیدی یادگیری ماشینی افزایش دهد. یادگیری ماشینی را می توان برای تصمیم‌گیری در مورد سطح ایمنی برنامه‌ها و جداسازی آنها از سایر برنامه‌های کاربردی در محیط تولید با کاهش سطح ایمنی قرار داد. سازمان‌ها را می‌توان برای پیش‌بینی، شناسایی و واکنش به رفتارهای غیرقانونی ناشی از ادغام هوش مصنوعی و یادگیری ماشینی توانمند نمود. نقاط محلی، اجرای اسکن‌های آنی هر فرآیند با شهرت ناآشنا را می‌توان با راه‌حل‌های هوش مصنوعی انجام داد و با یادگیری ماشینی برای ارتقای امنیت قدرت گرفت. یادگیری ماشینی می‌تواند با مشاهده‌ی رفتارهای مربوط به دسترسی به داده و انتقال داده، اطمینان حاصل کند که نقاط پایانی با الزامات نظارتی و سیاست‌های سازمانی مطابقت دارند.



نمودار ۱- سیستم امنیتی نقطه‌ی پایانی مبتنی بر هوش مصنوعی

این نمودار رابطه‌ی ماهیتی، یک سیستم امنیتی نقطه پایانی مبتنی بر هوش مصنوعی را نشان می‌دهد که در آن چندین دستگاه مانند رایانه، تلفن همراه و دستگاه‌های اینترنت اشیا به یک سیستم هوش مصنوعی مرکزی متصل هستند که آنها را نظارت و محافظت می‌کند.

هر دستگاه بطور منحصربفرد با یک شناسه‌ی دستگاه شناسایی می‌شود و بر اساس نوع دستگاه (مانند رایانه، تلفن همراه، اینترنت اشیا) با یک نام دستگاه خاص دسته‌بندی می‌شود. این دستگاه‌ها به سیستم AI متصل هستند که با ماهیت AI_System نشان داده شده و دارای شناسه منحصر بفرد خود aiSystemID و نام aiSystemName است. سیستم هوش مصنوعی بطور مداوم جریان‌های داده‌ی بلادرنگ ارسال شده با دستگاه‌های متصل را نظارت می‌کند. این جریان‌های داده با ماهیت DATA_Stream نشان داده می‌شوند که شامل dataStreamID برای شناسایی منحصربفرد هر جریان، نوع داده در حال تجزیه‌وتحلیل (dataType) و کلیدهای خارجی (aiSystemID و deviceID) است و جریان داده را به سیستم هوش مصنوعی و دستگاه اصلی مرتبط می‌کند.

سیستم هوش مصنوعی همچنین تضمین می‌کند که هر دستگاه با پروتکل‌های امنیتی خاصی که توسط نهاد Security_Protocol ارائه شده، مطابقت دارد. این ماهیت شامل یک شناسه‌ی پروتکل برای شناسایی منحصر بفرد، یک پروتکل Name، و یک وضعیت سازگاری است که نشان می‌دهد آیا دستگاه به پروتکل پایبند است یا خیر. سیستم هوش مصنوعی با اجرای این پروتکل‌ها در همه‌ی دستگاه‌های متصل، نقش مهمی در تضمین انطباق دارد. روابط موجود در نمودار نشان می‌دهد

که چگونه دستگاه‌ها داده‌ها را به سیستم هوش مصنوعی می‌فرستند که سپس این جریان‌های داده را نظارت می‌کند و از انطباق امنیتی اطمینان حاصل می‌کند و بنابراین از دسترسی غیرمجاز و حفظ یکپارچگی شبکه جلوگیری می‌نماید.

طبقه‌بندی تهدید

با افزایش چالش‌ها در امنیت سایبری، سازمان‌ها متوجه می‌شوند که هوش مصنوعی می‌تواند ارزش فوق‌العاده‌ای در دوره‌ی عملیات امنیتی روزانه بیافزاید. حوزه‌های متعددی از امنیت سایبری وجود دارد که هوش مصنوعی می‌تواند آن‌ها را افزایش دهد و در حال حاضر با استفاده از سرمایه‌ی انسانی شدید مدیریت می‌شوند. تهدیدات سایبری جدید را می‌توان توسط هوش مصنوعی از طریق تجزیه‌وتحلیل رفتاری داده‌های تولید شده در یک سازمان توسط شبکه‌ها، منابع محاسباتی، برنامه‌های کاربردی، منابع داده و کنترل‌های امنیتی به منظور تسهیل واکنش سریع به تهدیدات کشف کرد. از آنجایی که سطح حمله از جمله ابر (cloud)، دستگاه‌های تلفن همراه، دستگاه‌های اینترنت اشیا و همچنین شبکه‌های کلاسیک و نقاط پایانی محاسباتی همچنان در حال افزایش است، سازمان‌ها موظف هستند مجموعه‌ی بزرگ‌تری از کنترل‌های امنیتی را با افزودن الزامات نظارتی جدید ایجاد نمایند. مقدار داده‌های تولید شده از سطح حمله گسترده‌تر و کنترل‌های امنیتی وسیع‌تر به منظور فعال کردن نظارت نیز به طور قابل‌توجهی افزایش یافته که نیازمند تعهد زمانی بالا از سوی پرسنل امنیتی به منظور شناسایی رفتارهای عاملان تهدید و الگوهای مرتبط با ترافیک حمله است.

از آنجایی که پرسنل امنیتی موجود و زمان، منابع محدودی برای نظارت بر کنترل‌های امنیتی مختلف هستند، هوش مصنوعی می‌تواند محدودیت‌های منابع را تقویت کند تا با انجام فیلتر کردن داده‌ها، حذف موارد مثبت کاذب و نیز افزایش خود داده‌ها، شناسایی تهدیدات را خودکار کند و تا حد زیادی مشکلات تجزیه‌وتحلیل مقادیر زیادی از داده‌های مورد نیاز برای استراتژی-های فعلی عملیات امنیتی را کاهش دهد. راه‌حل‌های هوش مصنوعی، اتوماسیون پیشرفته‌ای را با کارایی بیشتر فراهم می‌کنند که پرسنل امنیتی را برای کار بر روی سایر مسئولیت‌های حیاتی آزاد می‌کند. کشف یک طرح جدید برای فعالیت‌های مخرب می‌تواند با نقشه‌های قبلی نامطلوب مرتبط باشد تا احتمال اینکه داده‌ها با هدف غیرقانونی با کارایی و دقت بیشتری نسبت به پرسنل امنیتی انجام دهند، مشخص شود. تجزیه‌وتحلیل همچنین می‌تواند توسط هوش مصنوعی انجام شود تا داده‌ها را از نقاط مبدا مختلف مرتبط کند و تصویری از اقدامات مخرب در حال انجام ایجاد شود تا پرسنل امنیتی بتوانند به طور کامل دامنه‌ی حمله را درک کنند.

تجزیه‌وتحلیل ریسک

پس از شناسایی یک تهدید، باید ارزیابی ریسک انجام شود بدین منظور که خطر واقعی تهدید با توجه به کنترل‌های امنیتی موجودی درک شود که در رأس تهدید شناسایی شده همپوشانی شدند. تشخیص این خطر به تیم‌های امنیتی این امکان را می‌دهد تا تأثیر بالقوه‌ی این تهدید را بر عملیات‌های سازمان درک کرده و به تیم پاسخگو اجازه می‌دهد تا مسیر مناسب اقدام مورد نیاز برای اصلاح را تعیین نماید. هوش مصنوعی با یادگیری ماشینی می‌تواند به فرآیند ارزیابی ریسک کمک کند؛ بدین منظور که واکنش مناسب به تهدید شناسایی شده با تشخیص زمینه‌ی مناسب جهت درک اکوسیستم امنیتی سازمانی فعلی را هدایت نماید.

راهنمای اصلاح

با استفاده از یادگیری ماشینی، راه‌حل‌های هوش مصنوعی می‌توانند عناوین و امضاهای امنیتی ایجاد کنند و آنها را به خودکفایی رسانده و کمتر به پیکربندی انسانی وابسته باشند و در عین حال در مسدود کردن تهدیدات جدید موفقیت بیشتری کسب کنند. پرسنل امنیتی قسمت اعظم زمان کاری خود را به کاربرد وصله‌ها اختصاص می‌دهند که در حال تبدیل شدن به

یک فرآیند بسیار خسته‌کننده از نظر زمان و مدیریت منابع است. هوش مصنوعی می‌تواند ریسک را از طریق پیاده‌سازی مدیریت وصله[1] کاهش دهد که اکتشاف، اولویت‌بندی و اصلاح آسیب‌پذیری‌ها را به استثنای کارهای دستی بیش از حد خودکار می‌کند. در محیط کنونی، پس از درک خطر راجع به تهدید، هشدارهای رویداد امنیتی در زمان واقعی را می‌توان با رویکردهای خودکار فعال کرد؛ بدین منظور که فعالیت‌های اصلاحی توسط انسان برای رسیدگی به مسائل امنیتی شناسایی شده در یک بازه‌ی زمانی معقول شروع گردد. همچنین می‌توان از یادگیری ماشینی برای تجزیه‌وتحلیل مناسب داده‌های مربوط به کنترل امنیتی به منظور شناسایی تهدیدها استفاده کرد، متعاقباً می‌توان از یادگیری ماشینی برای انجام پردازش‌های اساسی با نظارت و ارزیابی اقدامات قبلی انجام شده توسط تحلیلگران امنیت انسانی بهره برد. این آموزش موتور هوش مصنوعی می‌تواند توانایی سیستم را برای سازماندهی فعالیت‌های اصلاحی افزایش دهد. اقدامات تکرارشونده نیز می‌توانند توسط هوش مصنوعی و یادگیری ماشینی خودکار شوند. این مورد کاربردی، اعلان‌هایی را پوشش می‌دهد که اقدامات اصلاحی باید با خطر کم‌خطا تسریع شود و پلتفرم هوش مصنوعی در مورد تهدید اطمینان بالایی دارد. این قابلیت با توجه به کمبود کارشناسان باتجربه‌ی امنیت سایبری، سهولت و راحتی مورد نیازی را در صنعت فراهم می‌کند.

آینده‌ی نوآوری‌های هوش مصنوعی متعادل‌کننده‌ی امنیت سایبری

ادغام هوش مصنوعی و یادگیری ماشینی در امنیت سایبری، گام مهمی در مبارزه با تهدیدات سایبری پیچیده است. همانطور که این فناوری‌ها بیشتر در چارچوب‌های امنیتی می‌باشند، به نظارت استراتژیک نیاز اساسی دارند. این نظارت باید بر حفظ تعادل بین استفاده از قابلیت‌های پیشرفته‌ی هوش مصنوعی و حصول اطمینان از این متمرکز شود که استانداردهای اخلاقی یا یکپارچگی امنیتی سیستم‌ها را به خطر نمی‌اندازند. مکانیسم‌های نظارتی مؤثر ممکن است شامل مراحل آزمایش دقیق، نظارت مستمر بر رفتار هوش مصنوعی، و چارچوب‌هایی باشد که مسئولیت‌پذیری در تصمیم‌های مبتنی بر هوش مصنوعی را تضمین می‌کند. آینده‌ی امیدوارکننده‌ی هوش مصنوعی در امنیت سایبری به تحقیقات هدفمند با هدف پیشرفت مرزهای فناوری‌های فعلی و در عین حال رفع محدودیت‌های آنها بستگی دارد.

تحقیقات انجام شده در این خصوص می‌تواند این زمینه‌ها را بررسی نماید:

(۱) قابلیت‌های پاسخ خودکار: توسعه‌ی سیستم‌های هوش مصنوعی که نه تنها می‌تواند تهدیدها را شناسایی کند، بلکه به طور مستقل به آنها در زمان واقعی پاسخ داده و نیاز به مداخله‌ی انسانی را به حداقل می‌رساند؛

(۲) هوش مصنوعی متخاصم: بررسی روش‌هایی برای مقابله با حملاتی که در آن نهادهای مخرب از تکنیک‌های هوش مصنوعی برای تضعیف سیستم‌های امنیتی هوش مصنوعی استفاده می‌کنند؛

(۳) فناوری‌های حفظ حریم خصوصی: تقویت برنامه‌های هوش مصنوعی در امنیت سایبری با فناوری‌هایی که از حریم خصوصی کاربر محافظت می‌کنند، مانند یادگیری ترکیبی و حریم خصوصی متفاوت، که امکان بهبود مدل‌های هوش مصنوعی را بدون افشای داده‌های اساسی فراهم می‌کند.

علیرغم مزایایی که هوش مصنوعی برای امنیت سایبری به ارمغان می‌آورد، چالش‌های متعددی باقی می‌ماند که عبارتند از:

(۱) حفظ حریم خصوصی داده‌ها: از آنجایی که سیستم‌های هوش مصنوعی برای یادگیری و تطبیق به مقادیر زیادی داده نیاز دارند، اطمینان از حفظ حریم خصوصی و امنیت این داده‌ها بسیار مهم است. چالش در استفاده از داده‌ها برای آموزش هوش مصنوعی بدون به خطر انداختن محرمانه بودن و یکپارچگی اطلاعات نهفته است؛

---

[1]- patch management

(۲) آموزش مداوم و انطباق: مدل‌های هوش مصنوعی در امنیت سایبری به آموزش مداوم نیاز دارند تا در برابر تهدیدات در حال تحول موثر باقی بمانند. این فرآیند یادگیری مداوم باید مدیریت شود تا اطمینان حاصل شود که مدل‌ها قدیمی یا مغرضانه نمی‌شوند؛

(۳) خطرات دستکاری: این خطر وجود دارد که مهاجمان سایبری پیشرفته بتوانند سیستم‌های امنیتی مبتنی بر هوش مصنوعی را دستکاری کنند.

تحقیقات آینده نیاز به تمرکز بر توسعه‌ی سیستم‌های قوی دارد که می‌توانند چنین تلاش‌های دستکاری را شناسایی و کاهش دهند. پرداختن به این چالش‌ها مستلزم یک رویکرد متعادل است که نه تنها نوآوری‌های تکنولوژیکی را تحت فشار قرار می‌دهد، بلکه به شدت به استانداردهای اخلاقی و شیوه‌های امنیتی قوی پایبند است. همکاری میان نهادهای دانشگاهی، صنعتی و دولتی می‌تواند توسعه‌ی استانداردها و بهترین شیوه‌ها را تسهیل کند که استفاده‌ی اخلاقی از هوش مصنوعی را در امنیت سایبری راهنمایی می‌کند. با تمرکز بر این حوزه‌های استراتژیک، جامعه‌ی امنیت سایبری می‌تواند از پتانسیل هوش مصنوعی به طور مسئولانه و موثر استفاده کند و آینده‌ی دیجیتالی امن‌تری را تضمین کند.

نتیجه‌گیری

هوش مصنوعی به عنوان یک فناوری پیشرفته و قدرتمند، تأثیر بزرگی بر امنیت سایبری و حفاظت از داده‌ها دارد. از یکسو، هوش مصنوعی قادر است به صورت خودکار و با دقت بالا تهدیدات امنیتی را شناسایی کرده، الگوهای حملات را پیش‌بینی کرده و به صورت سریع واکنش مناسب را نسبت به حملات امنیتی نشان دهد. از سوی دیگر، استفاده از هوش مصنوعی ممکن است باعث نقض حریم خصوصی و پرهزینه شدن فرایندهای امنیتی شود. همچنین، خطرات احتمالی نظیر حملات به خود هوش مصنوعی نیز وجود دارد. با اینحال، با مدیریت مناسب و تعامل با تکنولوژی هوش مصنوعی، می‌توان بهبود قابل توجهی در امنیت سایبری و حفاظت از داده‌ها داشت. لذا، سازمان‌ها باید با دقت با استفاده از استانداردهای امنیتی مناسب، هوش مصنوعی را در سیستم‌های پیاده‌سازی کنند و به منظور کاهش خطرات احتمالی به مداوم آن را به روزرسانی کنند. به طور کلی، هوش مصنوعی می‌تواند نقش مهمی در تقویت امنیت سایبری و حفاظت از داده‌ها ایفا کند، اما نیاز به مدیریت مناسب و توجه به جنبه‌های امنیتی آن وجود دارد.

جایگاه هوش مصنوعی در امنیت سایبری به سرعت در حال توسعه است و اهمیت آن بیشتر و بیشتر می‌شود. روش‌های سنتی تشخیص و پیشگیری از تهدید دیگر کافی نیستند. سیستم‌های مبتنی بر هوش مصنوعی روش‌های پیچیده و پیشرفته‌ای را برای مقابله با حملات سایبری ارائه می‌کنند. برای شناسایی و متوقف کردن خطرات سایبری، سیستم‌های مبنی بر هوش مصنوعی از روش‌هایی مانند یادگیری ماشینی، یادگیری عمیق، پردازش زبان طبیعی، تجزیه‌وتحلیل پیش‌بینی‌کننده و تحلیل رفتاری استفاده می‌کنند. هوش مصنوعی قادر است به صورت خودکار و با دقت بالا تهدیدات امنیتی را شناسایی نموده و اقدامات مناسب برای مقابله با آنها را انجام دهد. با استفاده از الگوریتم‌های هوش مصنوعی، می‌توان الگوهای حملات سایبری را تشخیص داد و پیش‌بینی کرد تا اقدامات پیشگیرانه‌ی مناسب انجام شود. و همچنین هوش مصنوعی قادر است به صورت خودکار و سریع به حملات سایبری پاسخ دهد و از اطلاعات جمع‌آوری شده در زمان واقعی استفاده کند.

علاوه بر نقاط قوت فوق‌الذکر، استفاده از هوش مصنوعی در حفاظت از داده‌ها و امنیت سایبری نقاط ضعفی هم به همراه دارد. هوش مصنوعی نیز ممکن است به عنوان یک نقطه ضعف در سامانه‌های امنیتی مورد حمله قرار گیرد و توسط مهاجمان به سوءاستفاده تبدیل شود. استفاده از هوش مصنوعی در حفاظت از داده‌ها ممکن است باعث نقض حریم خصوصی کاربران شود و اطلاعات حساس آنها در خطر قرار گیرد. همچنین پیاده‌سازی و استفاده از تکنولوژی هوش مصنوعی در حفاظت از داده‌ها ممکن است هزینه‌بر باشد و برای برخی سازمان‌ها قابل دسترس نباشد. برای مدیریت و کنترل تأثیر هوش مصنوعی بر آزادی-

های اساسی و حقوق بشر، می‌توان از اتخاذ قوانین و مقررات برای محدود کردن استفاده از هوش مصنوعی در زمینه‌هایی که ممکن است به حقوق بشر و آزادی‌های اساسی آسیب بزند کمک گرفت و همچنین بررسی و نظارت منظم بر استفاده از هوش مصنوعی توسط سازمان‌های مستقل و قدرتمند به منظور جلوگیری از سوءاستفاده و تضمین رعایت حقوق بشر و اطلاع‌رسانی صحیح و شفاف از کاربرد هوش مصنوعی در تصمیم‌گیری‌ها و فرایندهای مختلف، به منظور افزایش اطمینان عمومی و کاهش نگرانی‌ها می‌تواند به مدیریت و کنترل تأثیر هوش مصنوعی بر حقوق بشر و آزادی‌های اساسی کمک کند و اطمینان حاصل کند که تکنولوژی همچنان به نفع انسان‌ها استفاده می‌شود.

حملات سایبری در حال افزایش است و آنها به طور فزاینده‌ای از هوش مصنوعی استفاده می‌کنند. در حالیکه هوش مصنوعی حتی می‌تواند به شرکت‌ها در مدیریت ریسک‌های امنیت سایبری کمک کند، باید شرایطی رعایت شود. با توجه به پیشرفت‌ها و چالش‌های ارائه شده توسط هوش مصنوعی در بخش مالی، به ویژه در امنیت سایبری و کشف تقلب، موارد زیر برای بررسی چشم‌انداز در حال تکامل می‌باشد:

اقدامات امنیت سایبری پیشرفته: موسسات مالی باید به طور مستمر استراتژی‌های امنیت سایبری خود را برای مقابله با تهدیدات مبتنی بر هوش مصنوعی اصلاح کنند. پیاده‌سازی ابزارهای پیشرفته هوش مصنوعی برای شناسایی و پاسخ به تهدیدات لازم و ضروری است. با اینحال، حفظ نظارت انسانی ماهر برای تفسیر دقیق داده‌های هوش مصنوعی و کاهش نادرستی‌ها یا سوگیری‌های بالقوه‌ی هوش مصنوعی به همان اندازه حیاتی است.

مکانیسم‌های پیشرفته تشخیص تقلب: این بخش باید به پذیرش مدل‌های هوش مصنوعی برای پیشگیری از تقلب ادامه دهد. پیشی گرفتن از کلاهبرداران ماهر از نظر فناوری مستلزم روش‌های پیشگیرانه‌ی شناسایی تقلب با هوش مصنوعی است، به ویژه استفاده از GenAI برای شناسایی زودهنگام و کاهش تقلب.

مقابله با هوش مصنوعی متخاصم: موسسات باید برای حملات پیچیده با قابلیت هوش مصنوعی، مانند تاکتیک‌های فیشینگ پیچیده و مهندسی اجتماعی، آماده شوند. سرمایه‌گذاری در سیستم‌های دفاعی جامع و بروزرسانی ابزارهای تشخیص تهدید برای مقابله با چالش‌های منحصربفرد هوش مصنوعی متخاصم، از جمله جعل‌های عمیق و اطلاعات نادرست، لازم و ضروری است.

استراتژی‌های مدیریت ریسک قوی: همسویی با چارچوب‌هایی مانند NIST AI RMF بسیار مهم است. موسسات مالی باید پروتکل‌های مدیریت ریسک خود را تقویت کنند و بر ریسک‌های نوظهور ناشی از افزایش دسترسی به هوش مصنوعی، به‌ویژه مدل‌های GenAI، که شامل موقعیت‌یابی داده‌ها و تعصبات مدل است، تمرکز نمایند.

همکاری و استانداردسازی در سراسر بخش: بخش مالی باید برای توسعه‌ی استراتژی‌های استاندارد شده برای مدیریت ریسک مرتبط با هوش مصنوعی همکاری کند. ایجاد دستورالعمل‌های خاص بخش مبتنی بر چارچوب‌های هوش مصنوعی می‌تواند به کاهش مؤثرتر تهدیدات نوظهور منجر شود و از همسویی با الزامات نظارتی و انتظارات نظارتی اطمینان حاصل کند.

سرمایه‌گذاری در تخصص انسانی: با درک نقش بی‌بدیل قضاوت انسان در برنامه‌های کاربردی هوش مصنوعی، سرمایه‌گذاری موسسات بر روی نیروی کار خود بسیار مهم است. برنامه‌های آموزشی و توسعه باید برای تجهیز کارکنان به مهارت‌های لازم برای کار موثر با فناوری‌های هوش مصنوعی اجرا شود.

مقررات مبتنی بر ریسک: تنظیم‌کننده‌ها باید نتایج و اهداف نظارتی روشن را شناسایی کنند، در حالیکه به نهادهای نظارت‌شده امکان می‌دهند تا تکنیک‌های مدیریت ریسک مؤثر را بر اساس استانداردها و بهترین شیوه‌های مشترک به کار گیرند.

نقش هوش مصنوعی در حوزه‌ها و برنامه‌های مختلف مورد توجه و چالش قرار گرفته است. با اینحال، حوزه‌ی امنیت سایبری عرصه‌ی حیاتی است که نمی‌تواند شکست تکنیک‌های هوش مصنوعی را تحمل کند زیرا امنیت تنها چیزی است که بین عوامل تهدید و اطلاعات و خدمات حساس وجود دارد. از اینرو محدودیت‌ها و نقاط قوت هوش مصنوعی برای محققان و توسعه‌دهندگان آینده لازم و ضروری می‌باشد تا تنظیمات و اصلاحات مناسب را برای تصمیم‌گیری مناسب انجام دهند. تکامل

هوش مصنوعی نیز برای راهنمایی محققان جهت درک جریان تغییراتی که منجر به فناوری هوش مصنوعی مدرن شده ارائه گردیده است و تغییرات را برای رساندن پتانسیل هوش مصنوعی به سمت جلو مرتبط می‌کند. نقاط قوت هوش مصنوعی را می‌توان با تکامل حملات سایبری حفظ نمود در صورتی که بتوان تکامل هوش مصنوعی را با همان سرعت حملات اجرا کرد. با توجه به امکان ادغام سایر فناوری‌ها در برنامه‌های امنیتی یکپارچه هوش مصنوعی، می‌توان از عوامل تهدید به طور مؤثر دفاع کرد یا حداقل تأثیر آن را کاهش داد. علاوه بر این، در مورد تغییر در سایر حوزه‌ها، هوش مصنوعی در امنیت سایبری نیروی کار را متحول می‌کند، آن را به سمت نقش‌هایی که از نظر فکری تقاضای بیشتری دارند هدایت نموده و نیاز به مجموعه مهارت‌های متنوعی دارد، در حالیکه فرصت‌هایی را برای رشد و انطباق در چشم‌انداز فناوری در حال تکامل ارائه می‌دهد.

در نهایت باید اذعان داشت که ادغام هوش مصنوعی در امنیت سایبری تنها یک گام تکاملی نیست؛ بلکه یک پاسخ ضروری به چالش‌های موجود در چشم‌انداز دیجیتالی مدرن است. با ادامه پیچیدگی و گسترش تهدیدات سایبری، تدابیر دفاعی نیز باید تکامل یابند. هوش مصنوعی راهکارهای نوآورانه و پیشگیرانه‌ای را معرفی می‌کند که به‌طور قابل‌توجهی توانایی بشر را در شناسایی، پیشگیری و پاسخ به نقض‌های امنیتی افزایش می‌دهد. با اینحال، سازمان‌ها باید به چالش‌های مرتبط با پذیرش هوش مصنوعی بپردازند و اطمینان حاصل کنند که ملاحظات اخلاقی، حریم خصوصی داده‌ها و شیوه‌های مؤثر اجرایی در اولویت استراتژی‌های آنها قرار دارد. با ادامه پیشرفت‌های تکنولوژیکی، همکاری بین هوش مصنوعی و امنیت سایبری به‌طور بیشتری پایه‌گذار یک آینده‌ی دیجیتالی ایمن‌تر خواهد بود.

منابع و مراجع

تقی‌زاده، مسلم و خردمندنیا، سهیلا، ۱۴۰۳، هوش مصنوعی مولد: چالش‌ها و الزامات توسعه و پیاده‌سازی. گزارش راهبردی، مرکز پژوهش‌های مجلس شورای اسلامی.

محمودی، امیررضا و بحرکاظمی، مریم، ۱۴۰۳، هوش مصنوعی و تأثیر آن بر امنیت سایبری و حق بر حریم خصوصی. فصلنامه‌ی پژوهش-های بنیادین در حقوق، اولین نشریه‌ی علمی تخصصی حقوق دانشگاه آزاد اسلامی واحد رفسنجان، ۱(۳)، ۸۵-۱۰۴.

Falowo, O.I.; Ozer, M.; Li, C.; Abdo, J.B. (۲۰۲٤). Evolving Malware and DDoS Attacks: Decadal Longitudinal Study. IEEE, ۱۲, ۳۹۲۲۱–۳۹۲۳۷.

Kapan, S.; Sora Gunal, E. (۲۰۲۳). Improved Phishing Attack Detection with Machine Learning: A Comprehensive Evaluation of Classifiers and Features. Appl. Sci, ۱۳, ۱۳۲٦۹.

Okdem, S.; Okdem, S. (۲۰۲٤). Artificial Intelligence in Cyber security: A Review and a Case Study. Appl. Sci, ۱۴, ۱۰۴۸۷. □□□□□://□□□.□□□/۱۰.۳۳۹۰/□□□۱۴۲۲۱۰۴۸۷.

Polona, C.; Tristan, M. (۲۰۲٤). Artificial intelligence and cyber security. EPRS (European Parliamentary Research Service), PE ۷٦۲,۲۹۲.

Razaulla, S.; Fachkha, C.; Markarian, C.; Gawanmeh, A.; Mansoor, W.; Fung, B.C.M.; Assi, C. (۲۰۲۳). The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE, ۱۱, ٤۰٦۹۸–٤۰۷۲۳.

Salama, R.; Al-Turjman, F. (۲۰۲۳). Cyber-Security Countermeasures and Vulnerabilities to Prevent Social-Engineering Attacks. In Artificial Intelligence of Health-Enabled Spaces; CRC Press: Boca Raton, FL, USA; pp. ۱۳۳–۱٤٤.

Temara, Sh. (۲۰۲٤). Harnessing the power of artificial intelligence to enhance next-generation cyber security. World Journal of Advanced Research and Reviews (WJARR), eISSN: ۲٥۸۱-۹٦۱٥, doi:۱۰,۳۰٥۷٤/wjarr.

U.S. Department of the Treasury. (۲۰۲٤). Managing Artificial Intelligence-Specific Cyber security Risks in the Financial Services Sector. AI Reports, pp: ۱-٥۲.