سازمان بهزیستی کشور

امنیت سایبری وهوش مصنوعی

در زیر ساخت های دولتی

معاونت آموزش و کارآفرینی جهاددانشگاهی استان زنجان

دوره های ضمن خدمت کارکنان بهزیستی

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 و 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.

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.

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.

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.

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.

برای مقابله با تهدیدات سایبری چه کارهایی می‌توان انجام داد؟

اصول امنیت سایبری برای سازمان‌های مختلف، شامل سازمان‌های دولتی، نظامی، قضایی، تجاری، صنعتی خصوصی و... تفاوت زیادی با همدیگر ندارند اما سطح حساسیت امنیت شبکه، داده‌ها و سیستم‌ها در سازمان‌ها با همدیگر تفاوت دارد و بر این اساس، سازمان‌ها می‌توانند میزان بودجه لازم برای تأمین امنیت سایبری و سخت‌گیری‌های لازم در ورود و خروج داده‌ها را سیاست‌گذاری کنند. پنج دسته از اقداماتی که هر سازمان برای جلوگیری از نفوذ و نشت داده‌ها باید انجام دهد، به شرح زیر هستند:

۱- آموزش اصول امنیت سایبری به پرسنل

همانطور که پیش از این گفتیم به دلیل دسترسی‌هایی که پرسنل سازمان‌ها به سامانه‌ها و شبکه‌های درون‌سازمانی دارند، می‌توانند اهداف مهمی برای هکرها به منظور نفوذ به سازمان‌ها باشند. در واقع، نفوذ به تلفن همراه یا رایانه پرسنل می‌تواند روشی برای نفوذ به سازمان باشد. همچنین، رعایت نکردن اصول امنیتی در هنگام اتصال به سامانه‌های درون سازمانی و استفاده از آن‌ها می‌تواند راه نفوذ را برای هکرها هموار کند. بنابراین، آموزش اصول امنیت سایبری به پرسنل از اهمیت بالایی برخوردار است و باید مورد توجه ویژه قرار گیرد.

همچنین سازمان‌ها باید:

- پرسنل را از تهدیدات سایبری متوجه سازمان آگاه سازند.
- کار با ابزارهای امنیتی همانند ضدویروس‌ها و EDRها، ابزارهای جمع‌آوری لاگ و... را به پرسنل آموزش دهند.
- مثال‌هایی واقعی از نفوذ و نشت اطلاعات و خسارت‌های وارده به سازمان‌ها و افراد به پرسنل ارائه دهند.
- از پرسنل نسبت به وضعیت امنیتی سازمان و نقاط ضعف آن بازخورد بگیرند.
- پرسنل را نسبت حملات فیشینگ و حملات مهندسی اجتماعی آگاه کنند.

۲- اهمیت حفاظت فیزیکی در تأمین امنیت سایبری

با اینکه که تهدیدات امنیتی و جرائم سایبری در دنیای امروز، اصلی‌ترین مسئله امنیتی برای سازمان‌ها هستند اما حفاظت فیزیکی نیز در حفظ امنیت سایبری نقش دارد. در واقع، سازمان‌های امروزی باید واحدهای حفاظت فیزیکی و امنیت سایبری خود را با هم دیگر ادغام یا حتی‌الامکان این واحدها را با همدیگر همگام و هماهنگ کنند.

در گذشته، اقدامات امنیت فیزیکی، شامل کنترل دسترسی، نظارت و آزمون، به عنوان عملیاتی مجزا از دیگر عملیات سازمان در نظر گرفته می‌شدند و در حفاظت فیزیکی، توجه زیادی به اهمیت داده‌ها و سیستم‌های ITو ارتباط متقابل آن‌ها با حفاظت فیزیکی نمی‌شد. متأسفانه، هنوز هم در بسیاری از سازمان‌هایی که تحت مدیریتی با تفکر سنتی قرار دارند، این تمایز قائل شدن بین حفاظت فیزیکی و امنیت سایبری، کاملا مشهود است.

حفاظت از داده‌های حساس و حریم خصوصی، بدون یک استراتژی ترکیبی حفاظت فیزیکی و امنیت سایبری، تقریبا غیر ممکن به نظر می‌رسد.

در این نوع استراتژی ترکیبی، دسترسی افراد به پایگاه‌های ذخیره‌سازی داده‌ها توسط اقدامات حفاظت فیزیکی محدود می‌شود و البته، می‌توان از اقدامات حفاظت سایبری برای محدود کردن دسترسی افراد به فضاهای فیزیکی مختلف در سازمان نیز کمک گرفت.

به عنوان مثال، نگهبانان واحد حفاظت فیزیکی می‌توانند جلوی دسترسی‌های غیرمجاز و فیزیکی افراد به پایگاه‌های داده و سرورها را بگیرند و متخصصان واحد امنیت سایبری نیز می‌توانند سیستم‌های احراز هویت برای کنترل دسترسی افراد به بخش‌های مختلف در سازمان، طراحی و پیاده‌سازی کنند.

۳- سطح‌بندی دسترسی و مدیریت هویت پرسنل

دسترسی پرسنل به سامانه‌ها و شبکه‌های درون‌سازمانی باید به صورت دقیق تعریف شود و هیچ کاربری نباید دسترسی غیرضروری داشته باشد. سطح‌بندی پرسنل و مدیریت هویت آن‌ها برای دسترسی به سامانه‌ها و شبکه‌های درون‌سازمانی از جایگاه ویژه‌ای در امنیت سایبری برخوردار است.

۴- استقرار سامانه‌های امنیتی

سازمان‌ها باید برای جلوگیری از نفوذ و مقابله با حملات هکری، سامانه‌های امنیتی قدرتمند و پیشرفته‌ای را مستقر کنند. این سامانه‌ها می‌توانند شامل سیستم‌های سخت‌افزاری و نرم‌افزاری برای نظارت بر ورود خروج داده‌ها و کنترل ترافیک شبکه باشند.

۵- پشتیبان‌گیری از داده‌ها

حتی در صورتی که تمام اصول امنیت سایبری به دقت رعایت شوند و سازمان مجهز به پیشرفته‌ترین سامانه‌های امنیتی برای پیشگیری از نفوذ باشد، احتمال نفوذ و هک شدن وجود داد. بنابراین، هر سازمانی باید به مدیریت بحران و بازیابی پس از حادثه اهمیت دهد و یکی از مهم‌ترین اصول پاسخگویی به حادثه، پشتیبان‌گیری از داده‌ها است.
بعد از هر حمله سایبری این احتمال وجود دارد که داده‌های حساس و ارزشمند آسیب ببینند و در نتیجه سازمان‌ها باید به طور پیوسته از داده‌ها پشتیبان‌گیری کنند تا در صورت آسیب دیدن آن‌ها، خسارات به حداقل برسد.

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:

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:

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 ((IoTنیز نقاط ورودی برای حملات ایمن‌سازی شبکه‌ها و دستگاه‌ها را افزایش می دهد.

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؟

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.

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.

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.

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:

۱- 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.

۲- 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.

۳- 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.

۴- 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.

۵- 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.

۶- 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.

۷- 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.

۸- 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.

۹- 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.

۱۰- 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.

۱۱- 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 IoTداشته 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.

۱۲- 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.

۱۳- 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.

۱۴- 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.

۱۵- 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.

۱۶- 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.

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:

۱- 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.

۲- 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.

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.

۳- 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.

۴- 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.

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:

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.

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.

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.

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.

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.

۴- 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.

۵- 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.

۶- 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.

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:

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.

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.

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.

آمار و احتمالات

روش‌های آماری و احتمالاتی برای تحلیل و پیش‌بینی تغییرات در داده‌ها و احتمال وقوع حوادث ناخواسته استفاده می‌شود.

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.

سیستم‌های تشخیص ناهنجار

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

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.